

PATENT
0717-0518P

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant: ZHANG, Xiaomang Conf.:
Appl. No.: NEW Group:
Filed: September 30, 2003 Examiner:
For: ELECTRONIC SEAL, MEMORY MEDIUM,
ADVANCED AUTHENTICATION SYSTEM, MOBILE
DEVICE, AND VEHICLE START CONTROL
APPARATUS

L E T T E R

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

September 30, 2003

Sir:

Under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55(a), the applicant(s) hereby claim(s) the right of priority based on the following application(s):

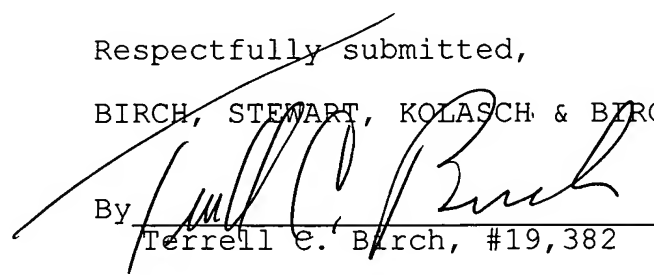
<u>Country</u>	<u>Application No.</u>	<u>Filed</u>
JAPAN	2002-289228	October 1, 2002

A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fee required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By 
Terrell E. Birch, #19,382

TCB/tmr
0717-0518P

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

Attachment(s)



ZHANG
BSK B LLP
703-205-8000
September 30, 2003
0717-0518P
1 OF 1

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 0 月 1 日
Date of Application:

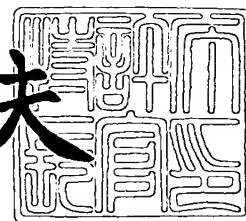
出 願 番 号 特 願 2 0 0 2 - 2 8 9 2 2 8
Application Number:
[ST. 10/C] : [J P 2 0 0 2 - 2 8 9 2 2 8]

出 願 人 シャープ株式会社
Applicant(s):

2 0 0 3 年 9 月 3 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 7 2 0 0 2

【書類名】 特許願

【整理番号】 02J02931

【提出日】 平成14年10月 1日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00
G07D 7/00

【発明者】

【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内

【氏名】 張 小▲忙▼

【特許出願人】

【識別番号】 000005049

【氏名又は名称】 シャープ株式会社

【代理人】

【識別番号】 100078282

【弁理士】

【氏名又は名称】 山本 秀策

【選任した代理人】

【識別番号】 100062409

【弁理士】

【氏名又は名称】 安村 高明

【選任した代理人】

【識別番号】 100107489

【弁理士】

【氏名又は名称】 大塩 竹志

【手数料の表示】

【予納台帳番号】 001878

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0208587

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子印鑑、リムーバブルメモリ媒体、事前認証システム、携帯機器、携帯電話装置および車両始動制御装置

【特許請求の範囲】

【請求項 1】 交信要求信号を生成する交信要求手段と、該交信要求信号を出力可能とすると共に、所定鍵に基づいて暗号化された乱数値を入力可能とする入出力手段と、該入出力手段で入力した乱数値を、所定鍵と関連した秘密鍵に基づいて復号した値を、該秘密鍵に基づいて暗号化する事前認証処理手段とを備え、該入出力手段は、事前認証処理手段で暗号化した乱数値を出力する電子印鑑。

【請求項 2】 前記事前認証処理手段は、
前記秘密鍵を記憶する秘密鍵記憶手段と、
該秘密鍵記憶手段の秘密鍵に基づいて、前記入出力手段によって入力された乱数値を復号する復号手段と、

該秘密鍵記憶手段の秘密鍵に基づいて、該復号手段によって復号化された乱数値を暗号化する暗号化手段とを有する請求項 1 記載の電子印鑑。

【請求項 3】 前記交信要求手段は、交信要求 I D (Identification) を記憶する交信要求 I D 記憶手段と、操作指令に基づいて該交信要求 I D 記憶手段内の交信要求 I D を交信要求信号として読み出すデータ読出手段とを有する請求項 1 記載の電子印鑑。

【請求項 4】 前記入出力手段は、相手側のリムーバブルメモリ媒体に対して電源供給可能とするリーダ／ライター装置である請求項 1 記載の電子印鑑。

【請求項 5】 前記所定鍵は公開鍵であり、前記秘密鍵は該公開鍵と R S A 暗号化方式または楕円曲線暗号化方式を用いて鍵ペアを構成する請求項 1 記載の電子印鑑。

【請求項 6】 交信要求信号を入力可能とする入出力手段と、該交信要求信号に基づいて起動信号を生成する起動信号生成手段と、該起動信号により所定鍵に基づいて乱数値を暗号化し、また、暗号化された乱数値を所定鍵に基づいて復号化して得られた値と該暗号化前の乱数値とが一致するかどうかを検出し、その検出結果を記憶する事前認証処理手段とを備え、該入出力手段は、該暗号化した

乱数値を出力可能とし、該暗号化された乱数値を入力可能とするリムーバブルメモリ媒体。

【請求項 7】 前記事前認証処理手段は、
乱数値を発生する乱数値発生手段と、
所定鍵を記憶する所定鍵記憶手段と、
該乱数値発生手段によって発生させた乱数値を前記起動信号により暗号化を開始すると共に、該所定鍵に基づいて暗号化する暗号化手段と、
該所定鍵に基づいて、所定鍵と関連した秘密鍵に基づいて暗号化された乱数値を復号する復号手段と、
該乱数値発生手段によって発生させた乱数値と該復号手段によって復号化された乱数値とを比較して一致するかどうかを検出する第 1 比較手段と、
該第 1 比較手段による検出結果を記憶する検出結果記憶手段とを有する請求項 6 記載のリムーバブルメモリ媒体。

【請求項 8】 前記起動信号生成手段は、交信要求 I D (Identification) を記憶する交信要求 I D 記憶手段と、相手側からの交信要求 I D と交信要求 I D 記憶手段内の交信要求 I D を比較して一致した場合のみ起動信号を出力する第 2 比較手段とを備えた請求項 6 記載のリムーバブルメモリ媒体。

【請求項 9】 前記入出力手段は、交信要求 I D を交信要求信号として受信可能とし、暗号化された乱数値を受信可能とする受信手段と、該暗号化した乱数値を相手側に送信可能とする送信手段とを有する請求項 6 記載のリムーバブルメモリ媒体。

【請求項 1 0】 前記所定鍵は公開鍵であり、前記秘密鍵は該公開鍵と R S A 暗号化方式または楕円曲線暗号化方式を用いて鍵ペアを構成する請求項 7 記載のリムーバブルメモリ媒体。

【請求項 1 1】 アクセス要求に対して、前記検出結果が一致を示す所定値の場合にアクセス許可信号を出力し、該検出結果が該所定値以外の場合にアクセス禁止信号を出力するアクセス許可処理手段を更に備えた請求項 7 記載のリムーバブルメモリ媒体。

【請求項 1 2】 前記アクセス許可処理手段は、前記所定値の場合にアクセ

ス許可信号を出力すると共に、前記検出結果記憶手段に前記所定値以外の値を前記検出結果として記憶させる請求項 1 1 記載のリムーバブルメモリ媒体。

【請求項 1 3】 請求項 1 記載の電子印鑑であって、少なくともメニュー画面および実行結果画面を表示可能とする表示部と、各種モードから所望のモードを選択可能とする選択・決定キーと、数字設定用キーと、選択モードを実行させるスタートキーとを有した電子印鑑。

【請求項 1 4】 外形形状がカード形状、円柱形状および角柱形状のいずれかである請求項 1 3 記載の電子印鑑。

【請求項 1 5】 前記所定鍵および秘密鍵からなる鍵情報を外部から 1 回に限り入力して関連メモリに設定可能とする初期設定モード部と、該関連メモリに格納した所定鍵を出力して届印処理する届印モード部とを有した請求項 1 記載の電子印鑑。

【請求項 1 6】 前記事前認証処理手段による事前承認結果を取り消すために取消信号を出力する取り消しモード部を有する請求項 1 記載の電子印鑑。

【請求項 1 7】 使用有効期間を関連メモリに設定可能とし、設定された使用有効期間を外部に出力する期間設定モード部を有する請求項 1 記載の電子印鑑。

【請求項 1 8】 使用有効回数を関連メモリに設定可能とし、設定された使用有効回数を外部に出力する回数設定モード部を有する請求項 1 記載の電子印鑑。

【請求項 1 9】 1 回に使うことができる金額の上限値を関連メモリに設定可能とし、設定された金額値を外部に出力する金額設定モード部を有した請求項 1 記載の電子印鑑。

【請求項 2 0】 前記表示部上に年月日時間を表示すると共に、前記数字設定用キーにより該年月日時間の時計表示の設定可能とする時計設定モード部を有した請求項 1 3 記載の電子印鑑。

【請求項 2 1】 外部から入力された所定鍵情報を登録処理する初期設定モード部を有した請求項 6 記載のリムーバブルメモリ媒体。

【請求項 2 2】 前記初期設定モード部は、請求項 1 5 記載の電子印鑑の届

印モード部による出力所定鍵情報を入力して関連メモリに設定する請求項 2 3 記載のリムーバブルメモリ媒体。

【請求項 2 3】 外部からの取消信号によって前記事前認証処理手段による事前承認結果を取り消す取り消しモード部を有する請求項 6 記載のリムーバブルメモリ媒体。

【請求項 2 4】 外部から入力された使用有効期間を関連メモリに設定可能とし、使用有効期間を超えるとアクセス許可処理を禁止する期間設定モード部を有する請求項 6 記載のリムーバブルメモリ媒体。

【請求項 2 5】 外部から入力された使用有効回数を関連メモリに設定可能とし、該設定回数を超えるとアクセス許可処理を禁止する回数設定モード部を有する請求項 6 記載のリムーバブルメモリ媒体。

【請求項 2 6】 1 回に使うことができる金額の上限値を外部から入力して関連メモリに設定可能とし、該設定金額を超えるとアクセス許可処理を禁止する金額設定モード部を有する請求項 6 記載のリムーバブルメモリ媒体。

【請求項 2 7】 請求項 1 ～ 5、1 3 ～ 2 0 の何れかに記載の電子印鑑と、請求項 6 ～ 1 2、2 1 ～ 2 6 の何れかに記載のリムーバブルメモリ媒体とを備え、該リムーバブルメモリ媒体と電子印鑑とが互いにデータ交換することにより事前認証処理を行う事前認証システム。

【請求項 2 8】 前記リムーバブルメモリ媒体は I C カードまたはメモリカードである請求項 2 7 記載の事前認証システム。

【請求項 2 9】 請求項 1 ～ 5、1 3 ～ 2 0 のいずれかに記載の電子印鑑が収納された携帯機器。

【請求項 3 0】 請求項 1 ～ 5、1 3 ～ 2 0 のいずれかに記載の電子印鑑が着脱自在に収納された携帯電話装置。

【請求項 3 1】 請求項 2 7 または 2 8 記載の事前認証システムにおいて、前記電子印鑑を収納した携帯機器と車体内の前記リムーバブルメモリ媒体との間で本人認証処理を前提として車の始動を可能とする車両始動制御装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、例えば市役所の窓口業務や電子商取引などで例えば I C カードやメモリカードなどに対して事前承認方式で本人認証を行う電子印鑑、これを使用可能とする I C カードおよびメモリカードなどのカード形式のリムーバブルメモリ媒体（着脱自在で携帯可能なメモリ媒体）、それらを用いた事前承認システム、この電子印鑑を収納した携帯機器、携帯電話装置および車両始動制御装置に関する。

【0 0 0 2】**【従来の技術】**

従来、市役所の窓口、商取引などにおいて、本人認証は印鑑（伝統印鑑）の捺印によって行われている。印鑑は、盗難などに遭った場合に気づき易いため、早急に被害防止対策を講じることができる。

【0 0 0 3】

近年では、I C カード、電子商取引、暗号化 E メールなどのように、情報が電子データ化（デジタルデータ化）されて流通されるようになってきており、それに伴って、本人認証の方法についても変化してきている。

【0 0 0 4】

I C カード、I D カード、電子商取引、暗号化 E メールなどにおいて、セキュリティ機能としては非常に強固なものが要求されるが、そのセキュリティ機能は、例えば 4 桁の暗証番号などのように、非常に脆弱な手段によって守られている。

【0 0 0 5】

例えば、電子財布として利用される I C カード（S m a r t C a r d とも称される）には、クレジットカードとキャッシュカードとがあり、クレジットカードの場合には I C カードによるセキュリティチェックと筆記署名の目視確認という二つの要素で本人認証が行われ、キャッシュカードの場合には I C カードによるセキュリティチェックと暗証番号の入力確認という二つの要素で本人認証が行われる。

【0 0 0 6】

しかしながら、模倣署名を目視判断で見破ることは容易ではなく、暗号番号は 4 桁の数字であるために安全性が低い。さらに安全性を高めるために、暗証データの桁数を増やすと、利用者の記憶に負担を強いることになる。

【 0 0 0 7 】

I C カードの安全性を高めるためには、署名、指紋、声紋、網膜パターン、顔などといった利用者固有の情報に基づいて本人認証を行う方法が考えられるが、そのアルゴリズムなどのソフト面や装置などのハード面からユーザ操作手数などの運営面までを考えると、それを I C カードが利用される現場で応用することは容易ではない。

【 0 0 0 8 】

また、I C カードは、主として欧米において、携帯電話器、ケーブルテレビジョン装置などの課金に対しても利用されており、そのセキュリティチェックは利用者に提供される P I N ナンバーによって行われている。このため、上記暗証番号と同様に、安全性の面で問題がある。

【 0 0 0 9 】

また、入退室管理カードのような I D カードは広く用いられているが、I D カードによって確認するだけで本人と認められることが多い。しかしながら、このような I D カードは、紛失・盗難などによって、簡単に悪用され得る。

【 0 0 1 0 】

また、電子商取引における安全性は、認証局によって証明書が発行された専用 W e b ブラウザに依存している。その専用 W e b ブラウザを利用するためには暗証番号が必要であるが、その暗証番号が漏れると、ブラウザ内部のセキュリティは強固であっても、誰でもアクセスすることができるようになる。

【 0 0 1 1 】

暗号化 E メールについては、暗号化関連の鍵などが計算機によって管理されているため、その計算機を利用する人であれば、自由に暗号化メールを読み書きすることができる。

【 0 0 1 2 】

図 1 3 は、従来の本人認証システムの一例を示すブロック図である。

【0013】

図13において、この本人認証システム110は、カード関連内容のバックアップをしている遠隔サーバ111と、例えば相関情報、セキュリティ処理情報および暗証番号照合情報などが記憶されたICカード112と、サービス内容表示処理、選択実行処理、セキュリティ処理および暗証番号入力処理などの各種処理を行うホストコンピュータ113と、ICカード112とホストコンピュータ113の交信インターフェイスおよび、非接触カードへの電源供給を行うとカードリーダー/カードライター114と、暗証番号などの入力装置115とを備え、ICカードをキャッシュカードとして用いる場合などに本人認証を行う。

【0014】

遠隔サーバ111には、ICカード112に関する情報がバックアップ保存されているが、遠隔サーバ111にアクセスするためにはリアルタイム通信が必要であるため、本人認証は、ICカード112とホストコンピュータ113の間および、ユーザとホストコンピュータ113の間で行われる。

【0015】

ICカード112およびホストコンピュータ113はセキュリティ機能を有しており、ICカード112が接触型である場合には、インターフェイスとしてのカードリーダー/カードライター114を介してICカード112とホストコンピュータ113との間で互いにセキュリティチェックのためにデータ交信が行われる。

【0016】

また、ICカード112が非接触型である場合には、カードリーダー/カードライター114からICカード112に対して電源が供給され、ホストコンピュータ113とICカード112との間で互いにセキュリティチェックのためにデータ交信が行われる。

【0017】

そのセキュリティチェックにおいて、ホストコンピュータ113がそのICカード112を真性であると確認すると、ホストコンピュータ113のディスプレイに暗証番号入力画面が表示される。

【 0 0 1 8 】

次に、ユーザによって暗証番号が入力装置 1 1 5 から入力されると、入力された暗証番号がホストコンピューター 1 1 3 からカードリーダー／カードライター 1 1 4 を介して I C カード 1 1 2 に供給され、I C カード 1 1 2 の内部で暗証番号の照合が行われる。この暗証番号の照合結果によって本人と確認されると、I C カード 1 1 2 の使用が認められる。ユーザによってサービス内容が選択されると、ホストコンピューター 1 1 3 によってそのサービスが実行されて、ホストコンピューター 1 1 3 のディスプレイにサービス内容が表示される。

【 0 0 1 9 】**【特許文献 1】**

特開平 3 - 9 2 9 6 6 号公報「電子財布システム」

【 0 0 2 0 】**【発明が解決しようとする課題】**

本発明者らが関連特許出願（特願 2 0 0 2 - 2 2 5 5 9 0 号）で提案した電子印鑑が I C カードの本人認証に使われる場合、その仕組みを図 1 3 および図 1 4 に示している。

【 0 0 2 1 】

図 1 4 は、本発明者らが関連特許出願で提案した本人認証システムの一実施形態における要部構成を示すブロック図である。

【 0 0 2 2 】

図 1 4 において、本人認証システム 2 0 0 は、遠隔サーバ 2 1 1 と、I C カードやメモリカードなどのカード 2 1 2 と、ホストコンピューター 2 1 3 と、カードリーダー・ライター 2 1 4 と、暗証番号などの入力装置 2 1 5 と、電子印鑑 2 1 6 とを有しており、カード 2 1 2 をキャッシュカードとして使う場合に電子印鑑 2 1 6 を用いて本人認証を行うようになっている。

【 0 0 2 3 】

遠隔サーバ 2 1 1 にはカード 2 1 2 の情報をバックアップして保存しているが、遠隔サーバ 2 1 1 のアクセスにリアルタイム通信が必要となる。このため、認証などのやり取りはホストコンピューター 2 1 3 とカード 2 1 2 と電子印鑑 2 1 6

との間で行われる。

【0024】

まず、ICカード212とホストコンピュータ213との間でセキュリティチェックを行う。お互いに認めてから、ホストコンピュータ213のディスプレイに対して暗証番号入力装置215から暗証番号を入力し、入力した暗証番号をカードリーダー・ライター214を経由してICカード212に送られ、ICカード212の内部で暗証番号の照合を行う。

【0025】

次に、ホストコンピュータ213はカードリーダー・ライター214を経由し、ICカード212に支払のための情報アクセス要求を出力する。ICカード212はホストコンピュータ213の情報アクセス要求に応じる前に、カードリーダー・ライター214を通して、電子印鑑216により本人であるかどうかを認証する本人認証を行う。ICカード212は電子印鑑216が本人の印鑑であると認めたら、ICカード212がホストコンピュータ213からの情報アクセス要求を許可する。また、ICカード212は電子印鑑216が本人の印鑑であると認めなかったら、ICカード212がホストコンピュータ213からの情報アクセス要求を拒否する。

【0026】

図15は、図14の本人認証システム200において電子印鑑により本人認証を行う際に、ICカードと電子印鑑との間に発生する処理内容を示すフローチャートである。

【0027】

図15に示すように、まず、ICカード212側からの乱数D1をランダムに生成する（ステップS301）。

【0028】

次に、生成された乱数D1と返信要求IDとを公開鍵Kpで暗号化した信号を、カードリーダー・ライター214を経由して電子印鑑216側に、カード会社のID番号と共に、公開鍵Kpで暗号化された乱数D1と公開鍵Kpで暗号化された返信要求IDとを送信する（ステップS302）。

【 0 0 2 9 】

さらに、電子印鑑 2 1 6 側では、受信したカード会社の I D 番号から秘密鍵 K s を特定する（ステップ S 3 0 3）。

【 0 0 3 0 】

さらに、公開鍵 K p で暗号化された乱数 D 1 と公開鍵 K p で暗号化された返信要求 I D とを、ステップ S 3 0 3 で特定した秘密鍵 K s で復号化する。これにより、復号化された送信要求 I D と復号化された乱数 D 2 とが得られる（ステップ S 3 0 4）。

【 0 0 3 1 】

さらに、復号された送信要求 I D が含まれているか否かを判断する（ステップ S 3 0 5）。判断した結果、送信要求 I D が含まれていない場合は、その時点で、処理を終了する（ステップ S 3 0 6）。また、判断した結果、送信要求 I D が含まれている場合には、複合化された乱数 D 2 をステップ S 3 0 3 で特定した秘密鍵 K s で暗号化して、暗号化された乱数 D 3 を I C カード側に送り返す（ステップ S 3 0 7）。

【 0 0 3 2 】

I C カード 2 1 2 側では、受信した暗号化された乱数 D 3 を公開鍵 K p で復号した乱数 D 3 を得る（S 3 0 8）。S 3 0 1 で生成した乱数 D 1 と S 3 0 8 で得られた乱数 D 3 との照合を行う（S 3 0 9）。照合した結果、一致であれば本人と認める（S 3 1 0）。照合した結果、不一致であれば、本人と認めない判断を下す（S 3 1 1）。

【 0 0 3 3 】

この本人認証システム 2 0 0 では、遠隔サーバー 2 1 1 に繋がるホストコンピュータ 2 1 3 と、I C カード 2 1 2 と、電子印鑑 2 1 6 との 3 者が揃うことが、本人認証を行う必要条件である。

【 0 0 3 4 】

即ち、I C カード 2 1 2 を使う度に電子印鑑 2 1 6 が使われるが、この場合の電子印鑑 2 1 6 とカードリーダー・ライター 2 1 4 との交信距離が遠距離（例えば 1 メートル以上）の場合には、電子印鑑 2 1 6 を I C カード 2 1 2 と一緒に提

出しなくても本人認証に支障を与えない。ところが、電波法の規制や省エネルギーにより非接触交信方式であっても交信距離は70cm以内である。このとき、交信を確実にを行うために、ICカード212をクレジットカードとして使う場合に、電子印鑑216をICカード212と一緒に操作店員さんに渡す必要が生じ、ICカード212の1枚だけ操作店員さんに渡す伝統的な従来の使い方に比べて操作手数が増える。

【0035】

また、電子印鑑216にカード会社のID番号を登録する必要がある。ICカード212を発行して貰うために、カード会社が電子印鑑216にその会社を識別するID番号を入力する。これにより、運営管理およびセキュリティの面で、色々な問題を生じる。運営管理の面においては、関連機関がカード会社や銀行を識別できるID番号の決定・公表・管理を実施することになり、これは莫大な作業である。カードを発行するとき、電子印鑑216にカード会社のID番号を組みこむことになり、本人認証の代わりに使う電子印鑑216へのデータの書き込みはセキュリティの観点から望ましくない。

【0036】

さらに、前述したように、遠隔サーバ211に繋がるホストコンピュータ213と、ICカード212と、電子印鑑216との3者が揃うことが、本人認証を行う上で必要条件であるため、認証フローが伝統的な電子印鑑を用いない場合に対してかなり変更を余儀なくされる部分がある。認証システムの変更により莫大な資金が必要となってしまう。

【0037】

さらに、電子印鑑216をメモリカードに保存したデータのアクセス保護に使用するときには、本人認証にはパーソナルコンピュータと、メモリカードと、電子印鑑216との3者が揃う必要がある。電子印鑑を用いない伝統的なシステムに、電子印鑑216と交信するためのカードリーダー・ライター214の増設、認証処理部分の追加などを行う必要が生じる。

【0038】

本発明は、上記従来の問題を解決するもので、電子印鑑にカード会社のID番

号を組み込むことなく、電子印鑑を届印としてカードに登録することにより、I Cカードを容易に発行でき、かつ、従来の電子印鑑を用いないシステムに対して新たなる改造や増設をすることなく、電子印鑑とカードによる事前の本人認証により処理相手に電子印鑑を渡さずに電子印鑑を高セキュリティでカードのアクセス保護に使用することができる電子印鑑、これを使用可能とするI Cカードおよびメモリカードなどのリムーバブルメモリ媒体、それらを用いた事前認証システム、この電子印鑑を収納した携帯機器、携帯電話装置および車両始動制御装置を提供することを目的とする。

【0 0 3 9】

【課題を解決するための手段】

本発明の電子印鑑は、交信要求信号を生成する交信要求手段と、交信要求信号を出力可能とすると共に、所定鍵に基づいて暗号化された乱数値を入力可能とする入出力手段と、入出力手段で入力した乱数値を、所定鍵と関連した秘密鍵に基づいて復号した値を、秘密鍵に基づいて暗号化する事前認証処理手段とを備え、入出力手段は、事前認証処理手段で暗号化した乱数値を出力するものであり、そのことにより上記目的が達成される。

【0 0 4 0】

また、好ましくは、本発明の電子印鑑における事前認証処理手段は、秘密鍵を記憶する秘密鍵記憶手段と、秘密鍵記憶手段の秘密鍵に基づいて、入出力手段によって入力された乱数値を復号する復号手段と、秘密鍵記憶手段の秘密鍵に基づいて、復号手段によって復号化された乱数値を暗号化する暗号化手段とを有する。

【0 0 4 1】

さらに、好ましくは、本発明の電子印鑑における交信要求手段は、交信要求ID (Identification) を記憶する交信要求ID記憶手段と、操作指令に基づいて該交信要求ID記憶手段内の交信要求IDを交信要求信号として読み出すデータ読出手段とを有する。

【0 0 4 2】

さらに、好ましくは、本発明の電子印鑑における入出力手段は、相手側のリム

ーバブルメモリ媒体に対して電源供給可能とするリーダ／ライター装置である。

【0043】

さらに、好ましくは、本発明の電子印鑑における所定鍵は公開鍵であり、秘密鍵は公開鍵とRSA暗号化方式または楕円曲線暗号化方式を用いて鍵ペアを構成する。

【0044】

本発明のリムーバブルメモリ媒体は、交信要求信号を入力可能とする入出力手段と、交信要求信号に基づいて起動信号を生成する起動信号生成手段と、起動信号により所定鍵に基づいて乱数値を暗号化し、また、暗号化された乱数値を所定鍵に基づいて復号化して得られた値と暗号化前の乱数値とが一致するかどうかを検出し、その検出結果を記憶する事前認証処理手段とを備え、入出力手段は、暗号化した乱数値を出力可能とし、暗号化された乱数値を入力可能とするものであり、そのことにより上記目的が達成される。

【0045】

また、好ましくは、本発明のリムーバブルメモリ媒体における事前認証処理手段は、乱数値を発生する乱数値発生手段と、所定鍵を記憶する所定鍵記憶手段と、乱数値発生手段によって発生させた乱数値を起動信号により暗号化を開始すると共に、所定鍵に基づいて暗号化する暗号化手段と、所定鍵に基づいて、所定鍵に関連した秘密鍵に基づいて暗号化された乱数値を復号する復号手段と、乱数値発生手段によって発生させた乱数値と復号手段によって復号化された乱数値とを比較して一致するかどうかを検出する第1比較手段と、第1比較手段による検出結果を記憶する検出結果記憶手段とを有する。

【0046】

さらに、好ましくは、本発明のリムーバブルメモリ媒体における起動信号生成手段は、交信要求ID (Identification) を記憶する交信要求ID記憶手段と、相手側からの交信要求IDと交信要求ID記憶手段内の交信要求IDを比較して一致した場合のみ起動信号を出力する第2比較手段とを有する。

【0047】

さらに、好ましくは、本発明のリムーバブルメモリ媒体における入出力手段は

、交信要求 I D を交信要求信号として受信可能とし、暗号化された乱数値を受信可能とする受信手段と、暗号化した乱数値を相手側に送信可能とする送信手段とを有する。

【 0 0 4 8 】

さらに、好ましくは、本発明のリムーバブルメモリ媒体における所定鍵は公開鍵であり、秘密鍵は公開鍵と R S A 暗号化方式または楕円曲線暗号化方式を用いて鍵ペアを構成する。

【 0 0 4 9 】

さらに、好ましくは、本発明のリムーバブルメモリ媒体において、アクセス要求に対して、検出結果が一致を示す所定値の場合にアクセス許可信号を出力し、検出結果が所定値以外の場合にアクセス禁止信号を出力するアクセス許可処理手段を更に備える。

【 0 0 5 0 】

さらに、好ましくは、本発明のリムーバブルメモリ媒体におけるアクセス許可処理手段は、所定値の場合にアクセス許可信号を出力すると共に、検出結果記憶手段に所定値以外の値を検出結果として記憶させる。

【 0 0 5 1 】

また、好ましくは、本発明の電子印鑑において、請求項 1 記載の電子印鑑であって、少なくともメニュー画面および実行結果画面を表示可能とする表示部と、各種モードから所望のモードを選択可能とする選択・決定キーと、数字設定用キーと、選択モードを実行させるスタートキーとを有する。

【 0 0 5 2 】

さらに、好ましくは、本発明の電子印鑑の外形形状がカード形状、円柱形状および角柱形状のいずれかである。

【 0 0 5 3 】

さらに、好ましくは、本発明の電子印鑑において、所定鍵および秘密鍵からなる鍵情報を外部から 1 回に限り入力して関連メモリに設定可能とする初期設定モード部と、この関連メモリに格納した所定鍵を出力して届印処理する届印モード部とを有する。

【 0 0 5 4 】

さらに、好ましくは、本発明の電子印鑑における事前認証処理手段による事前承認結果を取り消すために取消信号を出力する取り消しモード部を有する。

【 0 0 5 5 】

さらに、好ましくは、本発明の電子印鑑において、使用有効期間を関連メモリに設定可能とし、設定された使用有効期間を外部に出力させる期間設定モード部を有する。

【 0 0 5 6 】

さらに、好ましくは、本発明の電子印鑑において、使用有効回数を関連メモリに設定可能とし、設定された使用有効回数を外部に出力させる回数設定モード部を有する。

【 0 0 5 7 】

さらに、好ましくは、本発明の電子印鑑において、1回に使うことができる金額の上限値を関連メモリに設定可能とし、設定された金額値を外部に出力する金額設定モード部を有する。

【 0 0 5 8 】

さらに、好ましくは、本発明の電子印鑑において、表示部上に年月日時間を表示すると共に、数字設定用キーにより年月日時間の時計表示の設定可能とする時計設定モード部を有する。

【 0 0 5 9 】

また、好ましくは、本発明のリムーバブルメモリ媒体において、外部から入力された所定鍵情報を登録処理する初期設定モード部を有する。

【 0 0 6 0 】

さらに、好ましくは、本発明のリムーバブルメモリ媒体における初期設定モード部は、請求項 1 5 記載の電子印鑑の届印モード部による出力所定鍵情報を入力して関連メモリに設定する。

【 0 0 6 1 】

さらに、好ましくは、本発明のリムーバブルメモリ媒体において、外部からの取消信号によって事前認証処理手段による事前承認結果を取り消す取り消しモー

ド部を有する。

【 0 0 6 2 】

さらに、好ましくは、本発明のリムーバブルメモリ媒体において、外部から入力された使用有効期間を関連メモリに設定可能とし、この使用有効期間を超えるとアクセス許可処理を禁止する期間設定モード部を有する。

【 0 0 6 3 】

さらに、好ましくは、本発明のリムーバブルメモリ媒体において、外部から入力された使用有効回数を関連メモリに設定可能とし、この設定回数を超えるとアクセス許可処理を禁止する回数設定モード部を有する。

【 0 0 6 4 】

さらに、好ましくは、本発明のリムーバブルメモリ媒体において、1回に使うことができる金額の上限値を外部から入力して関連メモリに設定可能とし、この設定金額を超えるとアクセス許可処理を禁止する金額設定モード部を有する。

【 0 0 6 5 】

本発明の事前認証システムは、請求項 1 ～ 5、1 3 ～ 2 0 の何れかに記載の電子印鑑と、請求項 6 ～ 1 2、2 1 ～ 2 6 の何れかに記載のリムーバブルメモリ媒体とを備え、このリムーバブルメモリ媒体と電子印鑑とが互いにデータ交換することにより事前認証処理を行うものであり、そのことにより上記目的が達成される。

【 0 0 6 6 】

また、好ましくは、本発明の事前認証システムにおけるリムーバブルメモリ媒体は I C カードまたはメモリカードである。

【 0 0 6 7 】

本発明の携帯機器は、請求項 1 ～ 5、1 3 ～ 2 0 のいずれかに記載の電子印鑑が収納されたものであり、そのことにより上記目的が達成される。

【 0 0 6 8 】

本発明の携帯電話装置は、請求項 1 ～ 5、1 3 ～ 2 0 のいずれかに記載の電子印鑑が着脱自在に収納されたものであり、そのことにより上記目的が達成される。

。

【0069】

本発明の車両始動制御装置は、請求項27または28記載の事前認証システムにおいて、電子印鑑を収納した携帯機器と車体内のリムーバブルメモリ媒体との間で本人認証処理を前提として車の始動を可能とするものであり、そのことにより上記目的が達成される。

【0070】

上記構成により、以下、本発明の作用について説明する。

【0071】

まず、現状から順をおって説明する。例えば旧来の銀行のキャッシュカードや、ICカード、メモリカードなどのリムーバブルメモリ媒体としてのカード類を使う場合には、例えば4桁の暗証番号のみを予め決めておいて、ユーザがカードを使用するときに、そのカードを装置に挿入してから、この暗証番号を入力することで、本人認証を行っている。

【0072】

しかしながらこのような4桁の暗証番号では、コンピュータを用いて解析すれば、簡単にセキュリティを破られてしまう。つまり、現状の暗証番号による本人認証システムは、既に問題を抱えており、何らかの対策が必要な状況となっている。

【0073】

例えばICカードをクレジットカードとして使う場合には、通常は暗証番号さえ使わずに支払う様になっている。この時に、使用者に署名をさせることで、本人認証を行うことはできる。しかし、人が目視で署名の真偽を鑑別することは非常に困難である。即ち、現状ではICカードは本人でなくとも、これを取得した人は誰でも、何の不自由なく使用することが可能である。

【0074】

例えばメモリカード（例えばCF, Smart Media（登録商標）, SD, MemoryStick（登録商標）などと呼ばれているものなど）は近年、大容量かつ小型化になりつつあり、しかもその記憶内容は個人のプライバシー情報（顔写真、金融、証券、健康データ等）に深く関わっている。しかも、これら小型化のメモリカードは紛

失しやすく、容量が大きいので被害リスクが高くなる。現状においては、このようなメモリカードは、誰でもその内容を読み出すことが可能である。即ち、現状ではメモリカードのセキュリティ対策は十分に考慮されていない。

【 0 0 7 5 】

例えばキャッシュカードに関して、これらの問題に対する一つの解決策としては、暗証番号の桁数を大きくすることで、取り敢えずのセキュリティは確保できる。しかし、暗証番号の桁数は増やせば増やすほどセキュリティを破るのは難しくなり、その意味では望ましい方向であるが、桁数の多い暗証番号をユーザが覚えておくことは煩雑でもあり、更に暗証番号は度々変更しておかなければならないという事情があり、ユーザの使い勝手は悪くなるという問題点を持っている。同様に、クレジットカードやメモリカードに対しても、それなりのセキュリティ対策を講じる必要がある。

【 0 0 7 6 】

このようなカード類（ここでは単にカードと総称している）を使う上での事情を考慮して、一つのセキュリティを確保できるシステムとして、次に述べるようなものが提案された。それは基本的に述べると、本人認証のために、電子印鑑とカード（例えば IC カードまたはメモリカード、キャッシュカードなど）とホストコンピュータの、大きく分けて三つが揃って初めて、本人の認証が出来る前述した本人認証システム（特願 2 0 0 2 - 2 2 5 5 9 0 号）である。

【 0 0 7 7 】

ここで、電子印鑑は本人認証の為に使われるもので、イメージ的には IC カードに対する第 2 カードのようなものである。IC カードも電子印鑑も、暗号化された鍵情報を使って、本人認証を行う。従って、このように三つが揃って初めて、ユーザ本人がカードを使うことができるので、セキュリティ面では極めて安全とすることができる。

【 0 0 7 8 】

しかしながら、この本人認証システム（特願 2 0 0 2 - 2 2 5 5 9 0 号）には、次のような課題がある。つまり、この本人認証システムでは従来のカード使用のシステム構成を大幅に変更することになり、そのための設備投資が大掛かりに

なることと、ユーザにとっては一々カードと電子印鑑とを持ち歩かなくてはならないという使い勝手の悪さが課題としてある。

【0079】

そこで、本発明においては、このような従来のシステム自体を変更せずに、従来のカードシステムと共存できて、なおかつ高度なセキュリティを確保できる方式として、公開鍵と秘密鍵による鍵ペアを用いてカード（例えばＩＣカードまたはメモリカード、キャッシュカードなど）と電子印鑑とを直に交信可能とすることによりカード（例えばＩＣカードまたはメモリカード、キャッシュカードなど）を事前に電子印鑑で本人認証を行った上で、１回に限り使用できるようにしたものである。

【0080】

事前認証を行うための具体的構成について説明すると、電子印鑑およびカードは次のように構成されている。即ち、電子印鑑側からカードに対して交信要求（ＩＤ）を送信し、カードはこれをチェックする。チェックがＯＫであれば、カードの事前認証部分では、ランダム乱数を発生させ、これを公開鍵で暗号化して、電子印鑑側に送り、電子印鑑はこの受け取りデータを秘密鍵で復号化し、さらに秘密鍵で暗号化してＩＣカードに送る。このデータを受け取ったＩＣカードは、又公開鍵で復号化する。このときに、公開鍵データ（ＩＣカード側）と、秘密鍵データ（電子印鑑側）とは理論的に常に鍵ペアを構成している。乱数を暗号化して交信することも本発明の特長の一つである。

【0081】

例えばＩＣカードの場合、電子印鑑にその人しか持てない鍵情報を登録し、電子印鑑をカスタマイズする。登録は１回しか行なえない。未登録電子印鑑は鍵情報がオール１である。オール１であるときにのみ、登録が可能である。カスタマイズ済みの電子印鑑を届印として、金融機関に提出し、金融機関が電子印鑑に格納してある公開鍵情報を、ＩＣカードに登録してＩＣカードを発行して貰う。この登録も１回しか実施できない。また、電子印鑑側にカードリーダー・ライタと電池を内蔵すれば、電子印鑑とＩＣカードとの間で直に交信が可能となる。ユーザ本人だけでも、電子印鑑を使ってＩＣカードに事前の本人認証を行うことが可能

となる。このようにすれば、事前承認済みの I C カードが伝統的な I C カード金融システムでも使うことができる。もちろん、事前承認の無い I C カードは使えない。

【 0 0 8 2 】

例えばメモリカードの場合、カスタマイズ済みの電子印鑑を使って、ユーザ本人がメモリカードに電子印鑑の公開鍵を登録する。この登録も 1 回しか実施できないようにする。ユーザ本人が電子印鑑を使ってメモリカードに事前承認を行う。事前承認済みのメモリカードには汎用のパソコンなどでアクセスできる。もちろん、事前承認の無いメモリカードにはアクセスができない。メモリカードは従来のシステムで従来の通りに使用可能である。

【 0 0 8 3 】

このように、事前に本人認証を終えたカードは、一度だけホストコンピュータと交信できる。即ち一度だけなら、カード使用時点で事前の本人認証をせずにカードを使用できる。以後このカードは、使用の度に事前承認手続き（即ち、電子印鑑での承認）をしておけばよく、電子印鑑を持ち運ぶ必要がなくなる。

【 0 0 8 4 】

したがって、電子印鑑にカード会社の I D 番号を組み込むことなく、電子印鑑を届印としてカードに登録して I C カードを容易に発行でき、かつ、従来の電子印鑑を用いないシステムに対して新たな改造や増設をすることなく、相手に電子印鑑を渡さずに電子印鑑とカードによる事前の本人認証を行って、電子印鑑を高セキュリティでカードのアクセス保護に使用することが可能となる。

【 0 0 8 5 】

次に、この電子印鑑とは、「印鑑」という言葉があるので表現として誤解を与える可能性もあるが、要するに「個人認証のために、相手（ここではカード類）と鍵情報を用いて、データを乱数によって暗号化及び復号化処理することで交信して、個人認証を行う装置」である。この場合、装置がハンディ型で、簡単に持ち運びできることが重要で、第 2 のカードのようなものである。その意味では、電子印鑑の適用相手として、何もカード類に限る必要はなく、例えば販売機に対して直接電子印鑑で本人認証を行って、その場で物を購入できるようにしてもよ

いし（電子マネー）、有料テレビ、ゲーム機、電話装置などで使えるようにすることもできる。さらには、今回の電子印鑑機能を、常日頃使用者が持ち歩いているような道具類、例えば携帯電話機（電子印鑑の普及を目的として携帯電話機に外部から組み込む場合など）、車のキー（車の盗難防止対策として用いる場合など）、腕時計、PDAなどに搭載しておけば、これらの道具に搭載された電子印鑑機能を使って個人認証を行うことができるので、使い勝手は格段に向上する。即ち、市場規模として非常に大規模になると考えられる。

【0086】

【発明の実施の形態】

以下に、本発明の事前認証システムの実施形態1，2について図面を参照しながら説明する。

（実施形態1）

図1は、本発明の事前認証システムの実施形態1における要部構成を示すブロック図である。なお、ここでは、各要部毎の動作を示すフローチャートをも示している。

【0087】

図1において、この事前認証システム1は、遠隔サーバ2と、ホストコンピュータ3（またはパーソナルコンピュータ；以下パソコンという）と、カードとの通信インターフェースである入出力手段としてのリーダー・ライター装置としてのカードリーダ／カードライタ4と、秘密鍵による本人認証機能を持つ電子印鑑5と、秘密鍵と鍵ペアの公開鍵による本人認証機能を持つリムーバブルメモリ媒体としてのICカードやメモリカードなどのカード6とを備えている。

【0088】

遠隔サーバ2には、各種カード関連情報がバックアップ保存されている。

【0089】

ホストコンピュータ3は、入力装置31による入力指示によりカード6に対してカードアクセス要求処理が為され、セキュリティ処理として本人であることが認められた場合のみ遠隔サーバ2やカード6内の個人情報などと通信可能となり、ユーザ選択実行処理後に所望のカード関連情報を、サービス内容出力処理とし

て画面表示させたりプリントアウトさせたりできるようになっている。この本人認証は、遠隔サーバ2にアクセスするためにはリアルタイム通信が必要であるため、ホストコンピュータ3、電子印鑑5およびカード6の3者間で行われる。即ち、詳細には後述するが、電子印鑑5とカード6間の公開鍵方式暗号技術によって本人認証が行われ、ホストコンピュータ3とカード6との間で本人であることが確認されると、カード6の使用が認められ、ホストコンピュータ3のディスプレイ上にサービス内容が表示可能とされる。ユーザによって入力装置31からサービス内容が選択されると、ホストコンピュータ3によってそのサービスが実行されるようになっている。

【0090】

カードリーダー／カードライタ4は、非接触／接触用のカード6への電源供給を行うと共に、例えばホストコンピュータ3とカード6との間で互いにセキュリティ処理のためにデータ通信が行われる。このカードリーダー／カードライタ4の一例について図2にその詳細構成を示している。

【0091】

図2は、図1のカードリーダー／カードライタ4の要部構成例を示すブロック図である。なお、このカードリーダー／カードライタ4はホストコンピュータ3とカード6間の通信インターフェースの他に、後述するが、別途、電子印鑑5に内蔵されて設けられており、電子印鑑5とカード6との間での通信インターフェースとしても働く。

【0092】

図2において、カードリーダー／カードライタ4は、変調回路41と、復調回路42と、アンテナ43と、不揮発性メモリ44と、信号処理装置45と、制御回路46と、入出力I/F回路47とを有しており、ホストコンピュータ3とカード6との間で非接触通信（無線による送受信）を担う。

【0093】

変調回路41は、信号処理回路45からの信号が所定のキャリア波に変調されてアンテナ43に供給される。例えば13.56MHzのキャリア波がASK（Amplitude Shift Keying）方式でアンテナ43から送信される。

【0094】

復調回路 42 は、アンテナ 43 からの所定のキャリア波を復調して信号処理回路 45 に供給する。

【0095】

信号処理装置 45 は、制御回路 46 からの制御に基づいて、カード 12 とホストコンピュータ 3（または電子印鑑 5）のデータ入出力が検出され、データ通信の際に送受信される信号が処理される。

【0096】

制御回路 46 は、内部に CPU（中央演算処理装置）およびメモリなどを有しており、不揮発性メモリ 44 に予め記録されている制御プログラムを読み込んでそれを起動させることにより、カードリーダー／カードライター 4 を構成する各回路部を制御する。また、制御回路 46 は、入出力 I/F 回路 47 を介して、ホストコンピュータ 3 などの上位装置とのデータ通信が行われ、また、電子印鑑 5 に内蔵されているカードリーダー／カードライター 4 の場合には、電子印鑑 5 のセキュリティ処理部とのデータ通信が行われる。

【0097】

次に、電子印鑑 5 は、内蔵されたカードリーダー／カードライター 5A と、カードリーダー／カードライター 5A とデータ交信して事前認証処理を担う本発明の事前認証処理手段を構成するセキュリティ処理部 5B とを有している。なお、このカードリーダー／カードライター 5A は、前述したカードリーダー／カードライター 4 とその構成が同一であるため、ここではその説明を省略する。

【0098】

セキュリティ処理部 5B の一例について図 3 に詳細に示している。

【0099】

図 3 は、図 1 の電子印鑑 5 におけるセキュリティ処理部 5B の要部構成例を示すブロック図である。

【0100】

図 3 において、電子印鑑 5 のセキュリティ処理部 5B は、電源電圧を発生する電源部としての電池 51 と、交信要求 ID 記憶部 52 と、秘密鍵記憶部 53 と、

復号手段 54 と、暗号化手段 55 とを有している。

【0101】

電池 51 は、電子印鑑 5 の電源として用いると同時に、カードリーダー／カードライタ 5A を通してワイヤレスでカード 6 に対して電源を提供する。

【0102】

交信要求 ID 記憶部 52 は交信要求手段を構成している。この交信要求手段は、交信要求 ID (Identification) を記憶する交信要求 ID 記憶手段と、操作指令に基づいて交信要求 ID 記憶手段内の交信要求 ID を交信要求信号として読み出すデータ読出手段とから構成されており、記憶した交信要求 ID を読み出して電子印鑑 5 側からカード 6 側に送り、カード 6 に対して電子印鑑 5 との交信を要求する。

【0103】

秘密鍵記憶部 53 は、後述する公開鍵と所定の鍵ペアを構成する秘密鍵情報を記憶しており、秘密鍵情報を各所定のタイミングで復号手段 64 および暗号化手段 65 に出力する。

【0104】

復号手段 54 は、カード 6 側が交信要求 ID による交信要求に応じて、詳細に後述するが公開鍵で暗号化し、送信してきた受信暗号化乱数の値を、秘密鍵記憶部 63 の秘密鍵を用いて復号する。

【0105】

暗号化手段 55 は、復号した乱数の値を再び暗号化する。復号した乱数の値を秘密鍵記憶部 64 の秘密鍵を使って再び暗号化して、カードリーダー／カードライタ 5A を通してカード 6 側に送信する。

【0106】

次に、カード 6 の内部構成の一例について説明する。

【0107】

カード 6 は、カードリーダー／カードライタ 4 (または 5A) と交信可能な入出力手段としての図 4 の送受信・整流・ロジック回路 6A と、本発明の事前認証処理手段としての図 5 のセキュリティ処理部 6B と、本発明のアクセス許可処理手

段としての図6のアクセス許可処理部6Cとを有している。この場合、カード6は、ICカードやメモリカードなど各種カード類が考えられる。電子印鑑5に従来のようにカード会社のID番号を組み込むことなく、電子印鑑5を届印としてカード6側に登録（鍵ペア）することにより、カード6を発行することができる。また、ICカードについては、事前承認処理が済んであれば、カード6内部のアクセス許可処理を意識しなくても従来通りに使える。そうでなければ、ホストコンピュータ3によってICカードの使用は拒否される。また、メモリカードについては、事前承認処理が済んであれば、従来通りにメモリへのアクセスができる。そうでなければ、ホストコンピュータ3によってメモリカードへのアクセスは拒否される。

【0108】

図4は、図1のカード6に内蔵する送受信・整流・ロジック回路6Aの要部構成例を示すブロック図である。

【0109】

図4において、カード6の送受信・整流・ロジック回路6Aは、アンテナ61と、整流回路62と、クロック抽出回路63と、復調回路64と、定電圧発生回路65と、パワーオンリセット回路56と、変調回路67と、内部ロジック68とを有し、カード6と電子印鑑5またはホストコンピュータ3との非接触交信を担っている。なお、これらのアンテナ61、整流回路52、クロック抽出回路63および復調回路64により入力手段（ここでは受信手段であるが、接触型の場合を含んでいる）が構成され、また、アンテナ61、整流回路62、変調回路67および内部ロジック回路68により出力手段（ここでは送信手段であるが、接触型の場合を含んでいる）が構成されている。これらの入力手段および出力手段（受信手段および送信手段）により入出力手段（送受信手段）を構成している。

【0110】

アンテナ61は送受信手段であり、カードリーダー／カードライタ4または5Aからの信号が受信され得ると共に、カード6からの出力信号がカードリーダー／カードライタ4または5A側に送信され得る。

【0111】

整流回路 62 では、アンテナ 61 を介して受信された信号を整流してクロック抽出回路 63 および復調回路 64 に出力し、また、変調回路 67 からの信号を整流してアンテナ 61 に出力する。

【0112】

クロック抽出回路 63 は、アンテナ 61 を介して受信されたカードリーダー／カードライタ 4 からのキャリア波から動作に必要なクロック信号が抽出され、内部ロジック回路 68 に出力する。

【0113】

復調回路 64 では、送受信手段であるアンテナ 61 を介して受信されたカードリーダー／カードライタ 4 からの信号が復調されて内部ロジック回路 68 に出力する。

【0114】

定電圧発生回路 65 では、定電圧を発生してパワーオンリセット回路 66 および内部ロジック回路 68 に出力する。

【0115】

パワーオンリセット回路 66 は、カード 6 の電源遮断／リセットを制御する回路であり、内部ロジック回路 68 に電源遮断／リセットのための制御信号を出力する。

【0116】

変調回路 67 では、内部ロジック回路 68 による制御に基づいて、所定のキャリア波が任意の波長に変調され、アンテナ 61 を介してカードリーダー／カードライタ 4 に送信される。

【0117】

内部ロジック回路 68 は、CPU（中央演算処理装置）および、ROM および RAM からなるメモリなどを有しており、カード 6 を構成する各回路を制御する。なお、以上のアンテナ 61 ～変調回路 67 の構成は、カードリーダー／カードライタ 4 または 5A とカード 6 とが非接触型で交信する場合の一例を示したが、この構成に限定されるものではなく、カードリーダー／カードライタ 4 または 5A とカード 6 とが接触型で交信する場合として、図 4 の以外の構成を用いることも

可能である。

【0118】

図5は、図1のカード6におけるセキュリティ処理部6Bの要部構成例を示すブロック図である。

【0119】

図5において、カード6側の事前承認処理部であるセキュリティ処理部6Bは、交信要求ID記憶部71と、比較手段72（第2比較手段）と、乱数発生手段73と、乱数記憶部74と、公開鍵記憶部75と、暗号化手段76と、復号手段77と、比較手段78（第1比較手段）と、比較結果記憶手段としてのFLAG記憶部79とを有している。

【0120】

交信要求ID記憶部71は、交信要求ID（Identification）を記憶する交信要求ID記憶手段と、交信要求ID記憶手段内の交信要求IDを読み出すデータ読出手段とから構成されている。なお、この交信要求IDは電子印鑑5側の交信要求ID記憶部52にも記憶させているが、交信要求IDの設計については暗号化した交信要求ID番号を使うことで、電子印鑑5の特定や実行の高速化に効果が得られる。例えば、全ての電子印鑑5の交信要求IDを例えば「Let's Start」とすると、秘密鍵により暗号化した「Let's Start」を交信要求IDとして電子印鑑5に登録する。暗号化した交信要求IDの内容は電子印鑑5毎に異なるので、電子印鑑5の特定を容易にでき、電子印鑑5とカード6との交信スタートが簡単に制御できる。また、暗号化した交信要求IDをそのまま使うことにより、復号の時間は不要となり、演算の高速化や省エネにも効果がある。

【0121】

比較手段72は、電子印鑑5から受信したデータ（交信要求ID）と交信要求ID記憶部71の交信要求IDとを比較し、その比較結果が一致すれば、暗号化手段75による暗号化処理を実行し、また、その比較結果が一致しなければ、セキュリティ処理を終了する。即ち、比較手段72は、電子印鑑5側からの交信要求IDと交信要求ID記憶手段71内の交信要求IDを比較して一致した場合の

み暗号化手段 76 に起動信号を出力する。これらの交信要求 ID 記憶部 71 および比較手段 72 により起動信号生成手段が構成されている。

【0122】

乱数発生手段 73 は乱数を発生する。この乱数発生は公知の擬似乱数発生方法（例えば FIPS PUB 186-2 に提案されているハッシュ関数 SHA-1 を用いた乱数発生方法）が使える。

【0123】

乱数記憶部 74 は乱数発生手段 73 で発生した乱数を格納する。

【0124】

公開鍵記憶部 75 は公開鍵情報を記憶する。

【0125】

暗号化手段 76 は、乱数記憶部 74 からの記憶乱数の値を、公開鍵記憶部 75 からの公開鍵で暗号化し、送受信・整流・ロジック回路 6A を経て電子印鑑 5 側に送信する。ここで用いる暗号化方式としては例えば後述の RSA が使える。

【0126】

復号手段 77 は、電子印鑑 5 側から受信したデータを復号する。この復号の際に公開鍵記憶部 75 の公開鍵情報を使う。

【0127】

比較手段 78 は、復号手段 77 で復号したデータを乱数記憶部 74 に記憶している乱数の値と比較し、その比較結果が一致すれば、事前承認が有効であると判断して FLAG 記憶部 79 に「1」を設定し、また、その比較結果が一致しなければ、事前承認は無効であると判断して FLAG 記憶部 79 に「0」を設定する。

【0128】

FLAG 記憶部 79 は事前承認の比較結果状態を、事前承認有効を示す「1」または事前承認無効を示す「0」で記憶する。

【0129】

図 6 は、図 1 のカード 6 におけるアクセス許可処理部 6C の要部構成例を示すブロック図である。

【0 1 3 0】

図 6 において、カード 6 のアクセス許可処理部 6 C は、外部バスロック手段 8 1 と、比較手段 8 2 と、外部バスロック解除手段 8 3 と、不揮発性メモリ 8 4 と、外部バス制御部 8 5 とを有している。

【0 1 3 1】

外部バスロック手段 8 1 は外部バスをアクセス（内部からのデータ書き込み、データ読み出し）不能にする。即ち、外部バスロック手段 8 1 は、ホストコンピュータ 3（または汎用パーソナルコンピュータ）から、内蔵する送受信・整流・ロジック回路 6 A を経由して、不揮発性メモリ 8 5 に対してアクセスしようとするときに、内蔵する送受信・整流・ロジック回路 6 A のパワーオンリセット回路 6 6 の信号をトリガーとして外部バス制御手段 8 5 を介して外部バスをロック状態とし、不揮発性メモリ 8 4 に対するアクセスを不能にする。

【0 1 3 2】

比較手段 8 2 は、外部バスロック手段 8 1 を実行した後に、F L A G 記憶部 7 9 の値が「1」であるかどうかをチェックし、F L A G 記憶部 7 9 内の値が「1」であれば、F L A G 記憶部 7 9 内に「0」を入れ、「1」を示す比較結果信号を外部バスロック解除手段 8 3 に出力し、F L A G 記憶部 7 9 内の値が「1」でなければ、「0」を示す比較結果信号を外部バスロック解除手段 8 3 に出力して処理を終了する。

【0 1 3 3】

外部バスロック解除手段 8 3 は、「1」を示す比較結果信号を比較手段 8 2 から受けた場合には、外部バス制御部 8 5 にロック解除信号を出力してカード 6 の外部バスのロックを解除し、また、「0」を示す比較結果信号を比較手段 8 2 から受けた場合には、外部バス制御部 8 5 にロック解除信号を出力せず、カード 6 の外部バスはロック状態のままとなる。

【0 1 3 4】

不揮発性メモリ 8 4 は I C カードやメモリカードなどのカード 6 にある保護すべきメモリ領域である。

【0 1 3 5】

外部バス制御部 8 5 はカード 6 の保護すべきメモリ領域と外部接続用 I / F との間に設けたバス制御部である。

【0 1 3 6】

ここで、電子印鑑 5 側の秘密鍵 K_s は、カード 6 側の公開鍵 K_p と論理的に関連しており、以下の各種暗号化方式により公開鍵 K_p と秘密鍵 K_s とは所定の鍵ペアを構成している。

(暗号化方式：R S A 方式)

公開鍵 K_p と秘密鍵 K_s の鍵ペアにおいて R S A 公開鍵暗号方式を採用する場合には、次のように鍵ペア K_p , K_s を決める。

【0 1 3 7】

ほぼサイズの等しい二つの異なる素数 p と q を用意し、次式で n を計算する。

$$n = p \times q, \quad p \neq q$$

$p - 1$ と $q - 1$ の最小公倍数 n_1 を計算する。

$$n_1 = \text{LCM}(p - 1, q - 1) \quad (2)$$

n_1 に素な e を求める。

$$\text{GCD}(e, n_1) = 1 \quad (3)$$

次に、 d を求める。式 (3) から e^{-1} が存在することが判る。

$$d = e^{-1} \bmod n_1 \quad (4)$$

鍵ペアの範囲は $1 < e, d < n_1$ である。

【0 1 3 8】

公開鍵 K_p は (e, n) 、秘密鍵 K_s は (d) である。

【0 1 3 9】

現在の計算機の計算能力において、鍵長 (n の 2 進ビットの長さ) は 1 5 3 6 であれば、安全である。

(暗号化方式：楕円曲線暗号方式)

公開鍵 K_p と秘密鍵 K_s の鍵ペアにおいて楕円曲線暗号を採用する場合には、次のように鍵ペア K_p , K_s を決める。

【0 1 4 0】

素数 p として、1 6 0 ビット長の 2 進素数をランダムに選ぶ。

【0141】

楕円曲線 E として、式 (5) の条件を満たすように、 a 、 b を選び楕円曲線が決まる。

$$(4a^3 + 27b^2 \neq 0 \bmod p) \quad (5)$$

生成元 G として、楕円曲線の生成元を一つ選ぶ。

$$G = (X_0, Y_0) \quad (6)$$

ランダムな自然数 a として、式 (7) で乱数を選んで、式 (8) で楕円曲線の点 G の倍数 A を求める。

$$a \in \{1, 2, \dots, \#E - 1\} \quad (7)$$

$$A = aG = (X_a, Y_a) \quad (8)$$

ここで、 $\#E$ は楕円曲線の位数である。

【0142】

公開鍵として $(E, p, \#E, G, A)$ 、秘密鍵として (a) である。

【0143】

【表1】

暗号方式および鍵情報

暗号方式	識別番号	公開鍵 K_p	秘密鍵 K_s
RSA	1	e, n	d
楕円曲線	2	$E, p, \#E, G, A$	a

上記公開鍵 K_p は、カード会社などのような関連組織に自由に利用してもらうことが便利である。一方、上記秘密鍵 K_s は、電位印鑑 5 の中に閉じ込められており、アクセスできないようになっているため、安全性を向上させることができる。

【0144】

上記構成により、以下、本実施形態 1 の事前認証システム 1 の動作を説明する。

【0145】

図 1 に示すように、まず、ステップ S 101 において、交信要求 ID 記憶部 52 に記憶された交信要求 ID を、電子印鑑 5 側に内蔵されたカードリーダー／カードライタ 5A からカード 6 側に送信して、カード 6 に対して電子印鑑 5 との直接交信を要求する。

【0146】

次に、ステップ S 102 では、カード 6 側において、電子印鑑 5 側から受信した交信要求 ID を交信要求 ID 記憶部 71 内の交信要求 ID と比較し、その比較結果が一致しなければ（NO）、ステップ S 103 で処理を終了し、また、その比較結果が一致すれば（YES）、ステップ S 104 の処理に移行する。

【0147】

ステップ S 104 では、乱数発生手段 73 により乱数 D1 をランダムに生成して乱数記憶部 74 に記憶する。

【0148】

ステップ S 105 では、暗号化手段 76 により記憶乱数 D1 を公開鍵 Kp に基づいて暗号化する。その暗号化された乱数 D1 を、カード 6 側の送受信・整流・ロジック回路 6A から電子印鑑 5 側のカードリーダー／カードライタ 5A に送信する。

【0149】

電子印鑑 5 側では、ステップ S 106 において、受信された暗号化乱数 D1 を、復号手段 54 により秘密鍵 Ks に基づいて復号する。これによって、復号化された乱数 D2 が得られる。

【0150】

ステップ S 107 では、復号化された乱数 D2 を、暗号化手段 55 により秘密鍵 Ks に基づいて暗号化する。この暗号化された乱数を、電子印鑑 5 側のカードリーダー／カードライタ 5A からカード 6 側の送受信・整流・ロジック回路 6A に送信する。

【0151】

カード 6 側では、ステップ S 108 において、受信された暗号化乱数を、復号手段 77 により公開鍵 Kp に基づいて復号する。これによって、復号化された乱

数D3が得られる。

【0152】

ステップS109では、ステップS104で生成した記憶乱数D1とステップS108で得た乱数D3との照合を行う。この照合結果が一致した場合（YES）には、ステップS110の処理に進み、事前承認が有効であると判断してFLAG記憶部79に「1」を設定し、本人であると認める。

【0153】

また、ステップS109での照合結果が不一致であれば（NO）、ステップS111の処理に進み、事前承認は無効であると判断してFLAG記憶部79に「0」を設定し、本人として認めない。

【0154】

以上の一連の事前認証処理後（ステップS101～S111）に、ステップS121において、ホストコンピュータ3は、入力装置31からのユーザ入力によりカードアクセス要求を、カードリーダー／カードライター4を介してカード6側の送受信・整流・ロジック回路6Aに送信する。

【0155】

カード6側においては、外部バスロック手段81が外部バスをアクセス不能状態にして、不揮発性メモリ84に対してアクセスを不能にしている。このとき、ステップS122でFLAG記憶部79の値が「1」であるかどうかを比較手段72がチェックし、その値が「1」でなければ（NO）、ステップS123で「アクセス禁止」と判断して外部バスのロック状態を維持し、その旨を送受信・整流・ロジック回路6Aからカードリーダー／カードライター4を介してホストコンピュータ3側に送信する。ホストコンピュータ3側では、ステップS124で「カード6のアクセス不能」を検出して処理を終了する。

【0156】

ステップS122においてFLAG記憶部79の値が「1」であれば（YES）、ステップS125でFLAG記憶部79の値を「0」にリセットした後に、ステップS126で「アクセス許可」と判断して外部バスのロック解除を行い、その旨を送受信・整流・ロジック回路6Aからカードリーダー／カードライター4を

介してホストコンピュータ 3 側に送信する。ホストコンピュータ 3 側では、ステップ S 1 2 7 で「カード 6 のアクセス成功」を検出し、セキュリティ処理として本人であることが認められる。

【0157】

このような事前認証が成功した後に、ホストコンピュータ 3 と遠隔サーバ 2 とが交信可能となり、ユーザ選択実行処理後に遠隔サーバ 2 内の所望のカード関連情報を、サービス内容出力処理として画面表示させたりプリントアウトさせたりすることができる。

(実施形態 2)

上記実施形態 1 では、事前認証方式の電子印鑑 5 およびカード 6 を含む基本構成として事前認証システム 1 について説明したが、本実施形態 2 では、より機能の豊かな事前認証方式のマルチモード電子印鑑およびマルチモードカードを含む応用構成としてのマルチモード事前認証システムについて説明する。

【0158】

図 7 は、本発明の実施形態 2 におけるマルチモード事前認証システムの要部構成を示すブロック図である。

【0159】

図 7 において、このマルチモード事前認証システム 10 は、遠隔サーバ 2 と、ホストコンピュータ 3（またはパーソナルコンピュータ；以下パソコンという）と、カードとの交信インターフェースであるリーダー・ライター装置としてのカードリーダ／カードライタ 4 と、マルチモード電子印鑑 7 と、リムーバブルメモリ媒体としての IC カードやメモリカードなどのマルチモードカード 9 とを備えている。

【0160】

なお、このマルチモード事前認証システム 10 において、上記実施形態 1 の事前認証システム 1 と異なるのは、後述する図 8 および図 9 のマルチモード電子印鑑 7 および図 10 および図 11 のマルチモードカード 9 のように各マルチモード部が追加されている点であって、前述した遠隔サーバ 2、ホストコンピュータ 3（またはパーソナルコンピュータ；以下パソコンという）およびカードリーダ／

カードライタ 4, 7A の各構成部材の作用効果については上記実施形態 1 の場合と同様であるので、ここではその詳細な説明を省略する。

【0161】

マルチモード電子印鑑 7 は、図 7 に示すように、カードリーダー／カードライタ 7A と、セキュリティ処理部 7B（事前認証モード部 73）を含むマルチモード部とを有している。

【0162】

図 8 は、本発明の実施形態 2 におけるマルチモード事前認証システムのマルチモード電子印鑑の要部構成例を示すブロック図であり、図 9 は、図 8 のマルチモード電子印鑑の外観構成例を示す斜視図である。

【0163】

図 8 および図 9 において、マルチモード電子印鑑 7 は、マルチモード部として、初期設定モード部 71 と、届印モード部 72 と、事前承認モード部 73 と、取り消しモード部 74 と、時計モード部 75 と、期間設定モード部 76 と、回数設定モード部 77 と、金額設定モード部 78 と、時計設定モード部 79 と、LCD 表示部 80 と、選択キー 81 と、決定キー 82 と、カウンタキー 83 と、スタートキー 84 とを有している。

【0164】

初期設定モード部 71 は、電子印鑑 7 の鍵情報（公開鍵、秘密鍵などの情報）を外部から入力して設定する。この初期設定モード部 71 内の鍵情報記憶部（図示せず）への鍵情報の初期設定は、鍵管理センターや電気屋などで初期設定用の専用機器を使って行うようにすればよい。この初期設定が未実行の場合には鍵情報記憶部（図示せず）の記憶情報がオール「1」であるように設定し、このときのみ、鍵情報記憶部に対して鍵情報の初期設定処理を実行できるように構成する。即ち、初期登録に際して、登録許可レジスタが特定のデータ配列の時にのみ、鍵情報の暗号鍵データを入力できる構成になっている。その設定結果は、設定結果画面として初期設定モードの実行完了を示す「OK」または、初期設定不能を示す「NG」が LCD 表示部 80 上に表示され、これによってユーザに報知されるようにする。この制御は、図 2 に示すカードリーダー／カードライタ 7A におけ

る制御回路 46 内の CPU が介入し、選択キー 81 を使って LCD 表示部 80 上で各種モード表示から初期設定モードを選び、決定キー 82 のキー操作によって所望のモード、即ち初期設定モードを決定する。その後に、スタートキー 84 を押し続け、選択された初期設定モードが実行されて LCD 表示部 80 上に「OK」また「NG」が表示されたらスタートキー 84 を放せば初期設定モードが終了するようになっている。

【0165】

届印モード部 72 は、初期設定モード部 71 によって電子印鑑 7 内に格納している公開鍵を、後述するマルチモードカード 9 側に出力させて届印処理する。この届印モード部 72 の選択、決定、実行（スタート）、実行結果の表示確認は初期設定モード部 71 における上記一連の動作手順の場合と同じである。

【0166】

事前承認モード部 73 は、後述するマルチモードカード 9 に対して事前承認処理を行う。この事前認証処理と同時に、設定した期間・回数・金額の内容をカード 9 側に伝送する。カード 9 がメモリカードの場合に、メモリカードでは金額に関する内容がないので、メモリカードが受信した金額の内容が無視される。この事前承認モードの選択（選択キー 81）、決定（決定キー 82）、実行（スタートキー 84）、LCD 表示部 80 の実行結果画面の表示確認は初期設定モード部 71 における上記一連の動作手順の場合と同じである。

【0167】

取り消しモード部 74 は、上記事前承認結果を取り消すためのものである。この取り消しモードの選択、決定、実行、実行結果の表示確認は初期設定モード部 71 における上記一連の動作手順の場合と同じである。

【0168】

時計モード部 75 は、年月日時刻などの時情報を LCD 表示部 80 上で表示するモードである。電子印鑑 7 は特定操作がなければ、この時計モード部 75 による時計モードが自動的に選択されて、年月日時刻が表示画面上に表示されるようになっている。

【0169】

期間設定モード部 7 6 は、設定した日数を時計モード部 7 5 による日時と足し合わせてカード 9 側に送信するように動作するモードである。即ち、期間設定モード部 7 6 は有効期間（日数）の数値をカウンターキー 8 3 から入力し、その入力数値を関連メモリに記憶する。この登録データの書き換えは繰り返しできる。この期間設定モードは、選択キー 8 1 を使って各種モードから選択され、決定キー 8 2 を使って所望のモードに決定する。それから数字（日時）の設定はカウンタキー 8 3 を使って L C D 表示部 8 0 上で画面に表示された値を見ながら行うことができる。設定した数字（日時）を関連メモリ（例えば図 2 のカードリーダー／カードライタ 5 A における不揮発性メモリ 4 4 など）に記憶する。このモードの実行は電子印鑑 7 以外の機器に関係ないので、変調回路 4 1 と復調回路 4 2 を止めてもよい。

【 0 1 7 0 】

回数設定モード部 7 7 は、事前承認 1 回でカード 9 の使える有効使用回数を関連メモリに設定する。この登録データの書き換えは繰り返しできる。その設定方法は期間設定モード部 7 6 の場合と同じである。

【 0 1 7 1 】

金額設定モード部 7 8 は、I C カードに 1 回に使える金額の上限値を設定することができる。この登録データの書き換えは繰り返しできる。この設定方法も期間設定モード部 7 6 の場合と同じである。

【 0 1 7 2 】

時計設定モード部 7 9 は、年月日時間を合わせるためのモードである。この設定方法も期間設定モード部 7 6 の場合と同じである。

【 0 1 7 3 】

L C D 表示部 8 0 は、各種モードを表示する初期画面である設定メニュー画面、各種モードの実行結果を表示する実行結果画面などを表示可能である。L C D 表示部 8 0 を表示駆動するドライバ（図示せず）は、図 2 のカードリーダー／カードライタ 7 A における制御回路 4 6 に組み込まれている。

【 0 1 7 4 】

選択キー 8 1 は制御回路 4 6 の C P U を通してモードを選択する。

【0175】

決定キー 82 は制御回路 46 の CPU を通して選択したいモードを決定する。

【0176】

カウンタキー 83 は制御回路 46 の CPU を通して選択決定モードに数字設定があればこのキーを使って数字を設定する。

【0177】

スタートキー 84 は制御回路 46 の CPU を通してその押圧動作により実行を開始する。この場合、初期設定モード部 71、届印モード部 72、事前承認モード部 73、取り消しモード部 74 の四つのモードを実行する。その押圧動作を止めるとモードが終了する。

【0178】

以上のように、マルチモード電子印鑑 7 側に表 2 のマルチモードを設ける。

【0179】

【表 2】

電子印鑑のモード一覧表

モード	操作キー	処理内容	関連機器	確認方法
初期設定	選択、決定	鍵情報の登録	専用機器	LCD (OK, NG)
届印	選択、決定	公開鍵の出力	カード	LCD (OK, NG)
事前承認	選択、決定	承認と承認内容の出力	カード	LCD (OK, NG)
取り消し	選択、決定	承認の取り消し	カード	LCD (OK, NG)
期間設定	選択、決定、カウンタ	設定内容記録	なし	LCD (内容)
回数設定	選択、決定、カウンタ	設定内容記録	なし	LCD (内容)
金額設定	選択、決定、カウンタ	設定内容記録	なし	LCD (内容)
時計設定	選択、決定、カウンタ	時計の時間合わせ	なし	LCD (内容)

マルチモードカード 9 は、図 7 に示すように、図 4 の送受信・整流・ロジック回路 9A と、図 10 のセキュリティ処理部 9B を含むマルチモード部と、図 11 のアクセス許可処理部 9C とを有している。

【0180】

図 10 は、図 7 のマルチモードカード 9 におけるマルチモード部 9B の要部構

成例を示すブロック図である。

【 0 1 8 1 】

図 1 0 において、マルチモード部は、初期設定モード部 9 0 と、事前認証モード部 9 1 と、取り消しモード部 9 2 と、期間設定モード部 9 3 と、回数設定モード部 9 4 と、金額設定モード部 9 5 とを有している。

【 0 1 8 2 】

初期設定モード部 9 0 は、マルチモード電子印鑑 7 内の公開鍵を出力して生カード内に登録するための処理を行う。この処理はユーザ本人が行うことができる。例えばカード 9 を発行して貰うときに、身元確認のために電子印鑑 7 を届印として渡して、登録してもらうことも考えられる。同じカード 9 に対してこのモードを 1 回しか実行できないように構成している。このモードは電子印鑑 7 から受信した届印モードの ID 番号より識別される。カード 9 側が設定の結果「OK」または「NG」を電子印鑑 7 側に送信し、電子印鑑 7 側の LCD 表示部 8 0 上にこれを表示するようになっている。

【 0 1 8 3 】

事前認証モード部 9 1 は前述したような事前認証処理を行う。電子印鑑 7 との通信によりカード 9 の事前承認を許可または拒否する。このモードは電子印鑑 7 から受信した承認モードの ID 番号より識別される。カード 9 側が承認の結果「OK」または「NG」を電子印鑑 7 側に送信し、電子印鑑 7 側の LCD 表示部 8 0 上にこれを表示する。

【 0 1 8 4 】

取り消しモード部 9 2 は認証済みカード 9 に対して事前認証結果を取り消すためのモードである。まず、事前認証モード部 9 1 による事前認証処理を実行する。事前承認の結果が「OK」であれば、電子印鑑 7 が本物であり、事前承認を取り消し、「OK」を電子印鑑 7 側に送る。事前承認の結果が「NG」であれば、電子印鑑 7 は本物でなく、カード 9 の事前承認状態をそのまま維持し、「NG」を電子印鑑 7 側に送る。このモードは事前承認していないカード 9 に対しても、正しく実行できる。確実に事前認証を無効にするときに、このモードを実行すればよい。

【0185】

以上のマルチモードカード9側に表3のマルチモードを設ける。

【0186】

【表3】

カードのモード一覧表

モード	識別方法	処理内容	関連機器	確認方法
初期設定	印鑑側の届印モード	公開鍵の登録	電子印鑑	電子印鑑側
事前承認	印鑑側の承認モード	承認と承認内容の記録	電子印鑑	電子印鑑側
取り消し	印鑑側の取り消しモード	承認の取消	電子印鑑	電子印鑑側

図11は、図7のマルチモードカード9におけるアクセス許可処理部9Cの要部構成例を示すブロック図である。

【0187】

図11において、アクセス許可処理部9Cは、外部バスロック手段96と、FLAG記憶部79と、期間記憶部97と、カウントダウン・回数記憶部98と、比較手段99と、外部バスロック解除手段100と、不揮発性メモリ101と、外部バス制御部102とを有している。

【0188】

外部バスロック手段96は、外部バスをアクセス（書き込みまたは読み出し動作）不能にする。ホストコンピュータ3（または汎用パーソナルコンピュータ）からカードリーダー／ライター4さらに送受信・整流・ロジック回路9Aを経由して、不揮発性メモリ101にアクセスしようとするときに、送受信・整流・ロジック回路9Aのパワーオンリセット回路66からの信号をトリガーとしてカード9の外部バス制御部102をロック状態にし、不揮発性メモリ101へのアクセスを不能にする。

【0189】

期間記憶部97は有効期間を記憶するものである。

【0190】

カウントダウン・回数記憶部98は回数記憶部（関連メモリ；図示せず）に記憶している値から1を引き、その結果を回数記憶部に再度記憶する。図4のパワ

ーオンリセット回路 66 の信号をトリガーとしてこの処理を行う。

【0191】

比較手段 99 は、外部バスロック手段 96 によるバスロック処理を実行後に、FLAG 記憶部 79、期間記憶部 97、カウントダウン・回数記憶部 98 の各値をチェックし、FLAG 記憶部 79 の値が「1」であれば、比較処理を継続する。期間記憶部 97 の値がホストコンピュータ 3（または汎用パーソナルコンピュータ）から得た年月日時間と比較し、有効使用期間内であれば処理を継続する。カウントダウン・回数記憶部 98 の値をチェックし、正であれば外部バスロック手段 95 によるバスロック処理を実行する。FLAG 記憶部 79 の値が「0」であれば、処理を終了する。有効使用期間切れまたは回数記憶部の値が負であれば、FLAG 記憶部 96 に「0」を書く込んで処理を終了する。

【0192】

外部バスロック解除手段 100 は、カード 9 の外部バスのロックを解除する。

【0193】

不揮発性メモリ 101 は IC カードまたはメモリカードなどカード 9 にある保護すべきメモリ領域である。

【0194】

カード 9 の外部バス制御部 103 はカードの保護すべきメモリ領域（不揮発性メモリ 101）と外部接続用 I/F との間に設けたバス制御部である。

【0195】

金額記憶部 103 は、1 回に使える金額の上限値を記憶する。なお、金額記憶部 103 があるのは IC カードだけでありメモリカードにはこの記憶部はない。

【0196】

比較手段 104 は、不揮発性メモリ 101 から呼び出される金額の値を監視し、金額記憶部 103 の値を超えたら、カード 9 の外部バスをロック状態とし、カード 9 を使用不能にする。なお、比較手段 104 があるのは IC カードだけでありメモリカードにはこの比較手段 104 が存在しない。

【0197】

以上により、本実施形態 1，2 によれば、電子印鑑 5 または 7 側からカード 6


または 9 に対して交信要求 (ID) を送信し、カード 6 または 9 はこれをチェックする。チェックが OK であれば、カード 6 または 9 の事前認証部のカードセキュリティ処理部 6 B または 9 B では、ランダム乱数を発生させ、これを公開鍵で暗号化して、電子印鑑 5 または 7 側に送り、電子印鑑 5 または 7 はこの受け取ったデータを秘密鍵で復号化し、さらに秘密鍵で暗号化してカード 6 または 9 に送る。このデータを受け取ったカード 6 または 9 は、又公開鍵で復号化する。このようにして、事前に本人認証を終えたカード 6 または 9 は、一度だけホストコンピュータを介して遠隔サーバ 2 と交信できる。即ち一度だけなら、カード使用時点で事前の本人認証をせずにカード 6 または 9 をそのまま使用できる。以後このカード 6 または 9 は、使用の度に事前承認手続きをしておけばよく、電子印鑑 5 または 7 を持ち運ぶ必要がない。したがって、電子印鑑 5 または 7 にカード会社の ID 番号を組み込むこともなく、電子印鑑 5 または 7 を届印としてカード 6 または 9 に登録してカード 6 または 9 を容易に発行でき、かつ、従来の電子印鑑 5 または 7 を用いないシステムに対して新たな改造や増設をすることなく、処理相手に電子印鑑 5 または 7 を渡さずに、電子印鑑 5 または 7 を高セキュリティでカード 6 または 9 のアクセス保護に使用することができる。

【0 1 9 8】

なお、上記実施形態 1, 2 の電子印鑑 5 または 7 の応用可能な分野を図 1 2 に示している。図 1 2 における括弧の中の内容は、従来の本人認証方法を示している。

【0 1 9 9】

従来では、例えば、カードによる買い物を行う場合などには、署名を目視確認することにより本人認証が行われている。また、カードによる現金引き出し、携帯電話装置などによる遠隔家電制御、カードによる携帯電話装置などの課金、パーソナルコンピュータへのアクセス、電子錠の開錠を行う場合などには、暗証番号を入力することにより本人認証が行われている。また、入退室管理、給油・高速料の支払い、電車の乗車料金・公衆電話料金の支払いを行う場合などには、カードを確認することによって本人認証が行われており、カードの所持者は真性な利用者であると判断されている。また、車両防犯のためには、車両の鍵によって



本人認証が行われており、鍵の保持者は車両の真性な利用者であると判断されている。また、市役所の窓口などでは、伝統印鑑により本人認証が行われており、書き留め郵便配達の受け取りでは、伝統印鑑またはサインにより本人認証が行われている。また、高級家電の盗難防止については、個人が管理しているだけであり、本人認証による使用許可などは行われていない。

【 0 2 0 0 】

このような分野で、本発明の電子印鑑 5 または 7 を従来の認証方法と組み合わせることで、利用者に負担をかけずに、安全性を格段に向上させることができる。暗証番号は、盗難にあっても被害が発生しない限り発覚されないが、本発明の電子印鑑 5 または 7 は盗難にあったときに気が付き易く、被害防止対策を早急に行うことができる。また、電子印鑑 5 または 7 を紛失しただけでは、被害は生じにくい。

【 0 2 0 1 】

従来は、市役所の窓口などでの本人認証、書き留め郵便配達を受け取りには、伝統印鑑が用いられているが、今後、例えば国民総背番号制などのように、個人情報電子データ化され、そのデータを利用して情報・サービスが提供されると共に個人の権利・義務が管理されるような、いわゆる電子化政府になっていくことを考えると、本発明の電子印鑑 5 または 7 を伝統印鑑に変えて利用することは、非常に有効である。

【 0 2 0 2 】

また、高級家電製品などに本人認証機能を加えることによって、盗難を防止することができる。テレビジョンセット、冷蔵庫、ビデオ、カメラなどの電子機器に対して、本発明の電子印鑑 5 または 7 による本人認証機能を設けて、電源投入の際に本人認証を要求することによって、本発明の電子印鑑 5 または 7 が無いと、これらの電子機器が作動しないことになる。このような機能は、発展途上国において実効性がある。

【 0 2 0 3 】

さらに、定期券などの IC カードにおいて、本発明の電子印鑑 5 または 7 による本人認証機能を設けることによって、IC カードを紛失した場合の届率が高く

なると考えられる。

【0204】

特に、本発明の電子印鑑 5 または 7 を携帯電話装置に着脱自在に搭載し、本発明の電子印鑑 5 または 7 が携帯電話装置のインターフェースを共用するように構成することもできる。携帯電話装置の機種変更時に本発明の電子印鑑 5 または 7 を取り除いて、新たな機種の携帯電話装置の機種変更時に本発明の電子印鑑 5 または 7 を容易に取り付けることができるようにする。また、本発明の電子印鑑 5 または 7 の形状は電池のような円柱形状や角柱形状の他、カード形状であってもよい。

【0205】

また、車の盗難防止対策としても本発明の電子印鑑 5 または 7 を用いることができる。この場合に、本発明の電子印鑑 5 または 7 を車のキーと同様に用い、本発明のカード 6 または 9 の事前認証処理部のセキュリティ処理部 6 B または 9 B およびアクセス許可処理部 6 C または 9 C と、ホストコンピュータ 3 の各機能を車の制御部内に車両始動制御装置として搭載するようにしてもよい。

【0206】

【発明の効果】

以上のように、本発明によれば、カードに製造段階で電子印鑑により事前承認に関する機能を持たせることができる。

【0207】

また、電子印鑑を用いてカードで事前認証を行うため、従来のようにカードと電子印鑑を一緒に提出する必要がなく、カード使用時に、事前承認済みのカードだけを提出すればよい。ため、ユーザに負担かけることなく、カードのデータを確実に保護することができる。

【0208】

さらに、事前認証機能のあるカードは従来のシステム上に事前認証機能の無いカードと同様に使えるため、従来のシステムを新たに改造せずとも、そのまま使用することができる。

【図面の簡単な説明】

【図 1】

本発明の事前認証システムの実施形態 1 における要部構成を示すブロック図である。

【図 2】

図 1 のカードリーダー／カードライタ 4 の要部構成例を示すブロック図である。

【図 3】

図 1 の電子印鑑 5 におけるセキュリティ処理部 5 B の要部構成例を示すブロック図である。

【図 4】

図 1 のカード 6 に内蔵する送受信・整流・ロジック回路 6 A の要部構成例を示すブロック図である。

【図 5】

図 1 のカード 6 におけるセキュリティ処理部 6 B の要部構成例を示すブロック図である。

【図 6】

図 1 のカード 6 におけるアクセス許可処理部 6 C の要部構成例を示すブロック図である。

【図 7】

本発明の実施形態 2 におけるマルチモード事前認証システムの要部構成を示すブロック図である。

【図 8】

本発明の実施形態 2 におけるマルチモード事前認証システムのマルチモード電子印鑑の要部構成例を示すブロック図である。

【図 9】

図 8 のマルチモード電子印鑑の外観構成例を示す斜視図である。

【図 10】

図 7 のマルチモードカード 9 におけるマルチモード部 9 B の要部構成例を示すブロック図である。

【図 11】

図 7 のマルチモードカード 9 におけるアクセス許可処理部 9 C の要部構成例を示すブロック図である。

【図 1 2】

本発明の電子印鑑の応用可能な分野を示す図である。

【図 1 3】

従来 of 本人認証システムの一例を示すブロック図である。

【図 1 4】

本発明者らが関連特許出願で提案した本人認証システムの一実施形態における要部構成を示すブロック図である。

【図 1 5】

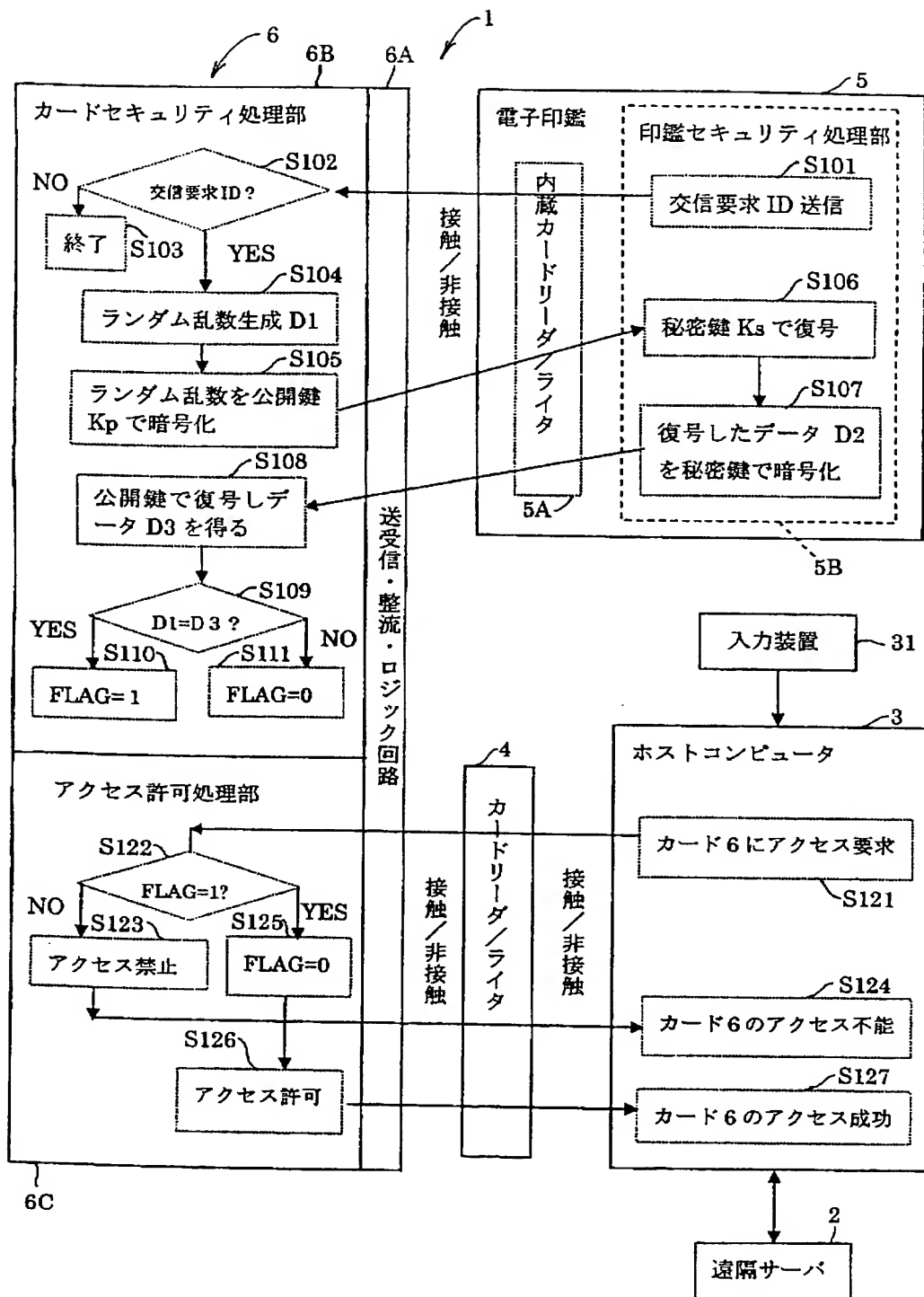
図 1 4 の本人認証システム 2 0 0 において電子印鑑により本人認証を行う際に、I C カードと電子印鑑との間に発生する処理内容を示すフローチャートである。

【符号の説明】

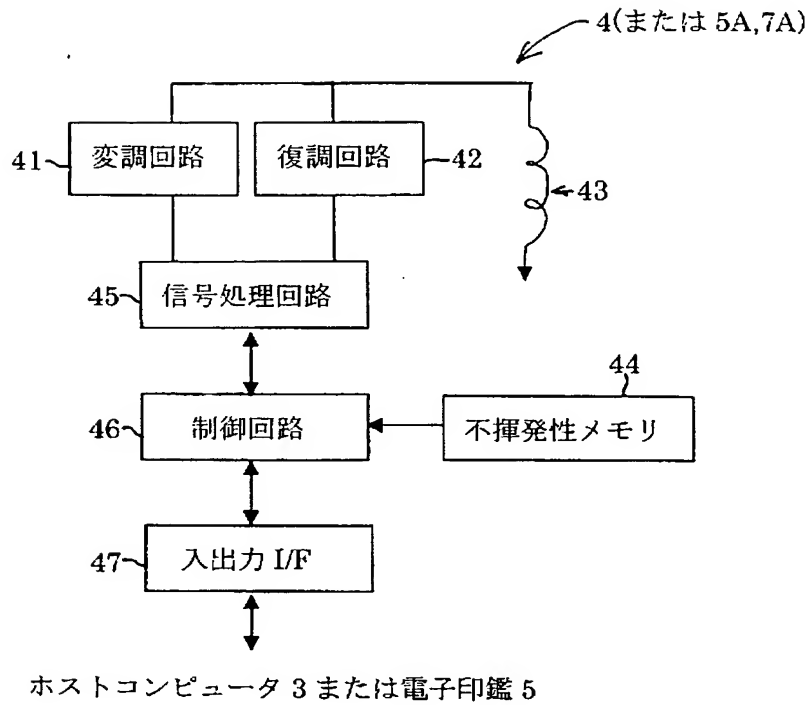
- 1 事前認証システム
- 2 遠隔サーバ
- 3 ホストコンピュータ
- 4, 5 A, 7 A カードリーダー／カードライター
- 5, 7 電子印鑑
- 6, 9 カード

【書類名】 図面

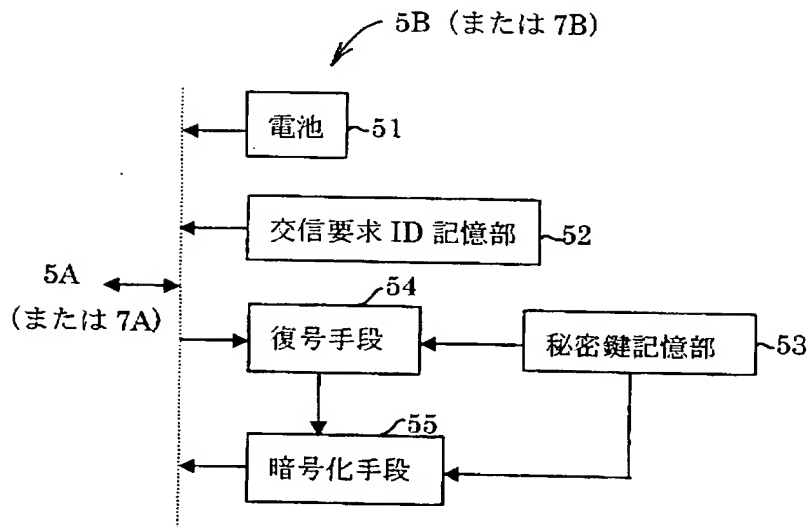
【図1】



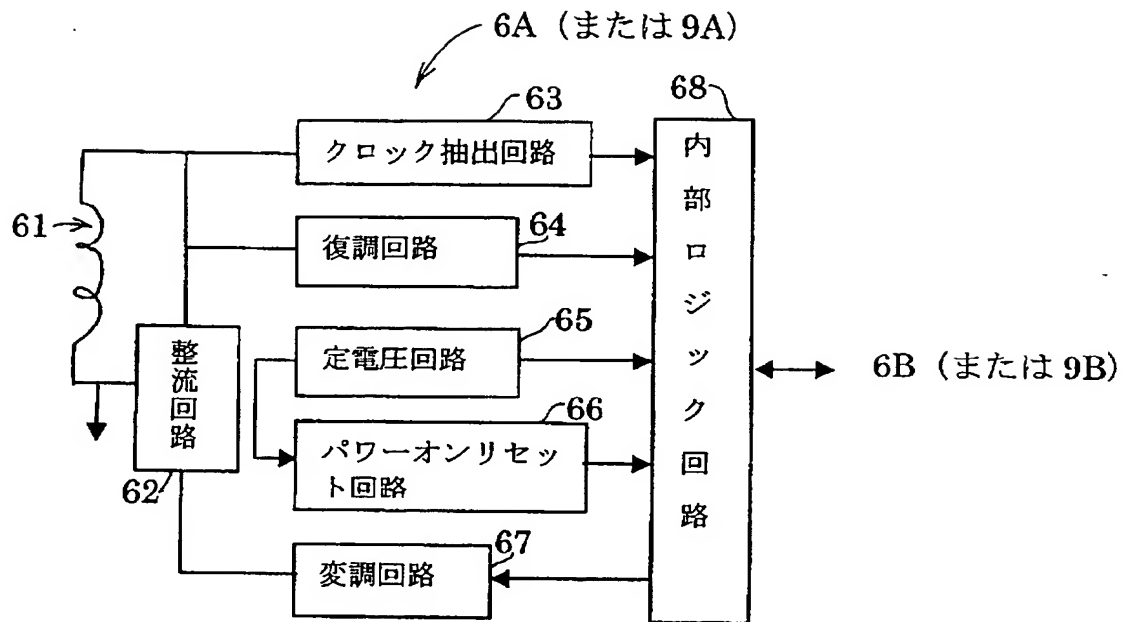
【図 2】



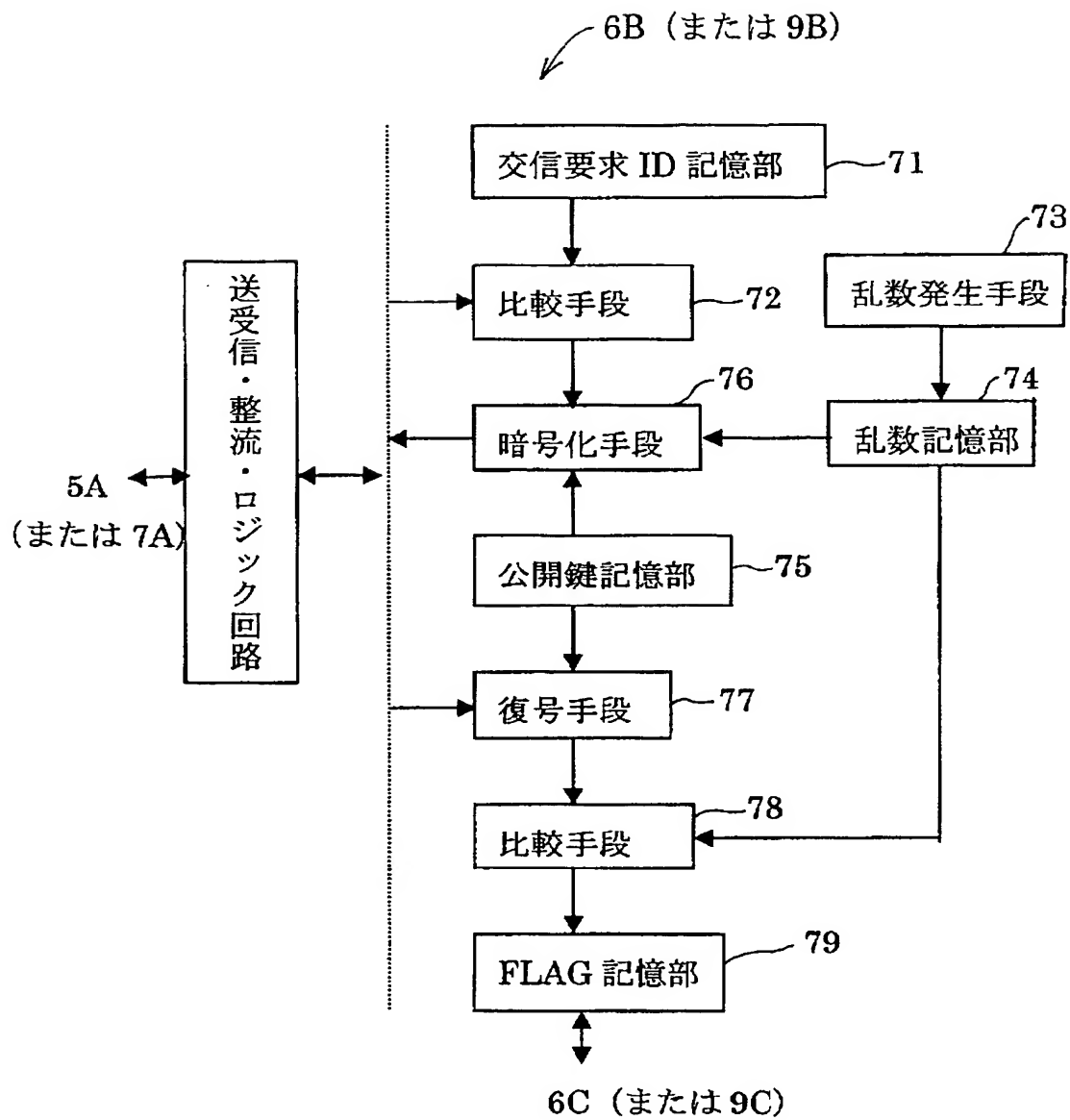
【図 3】



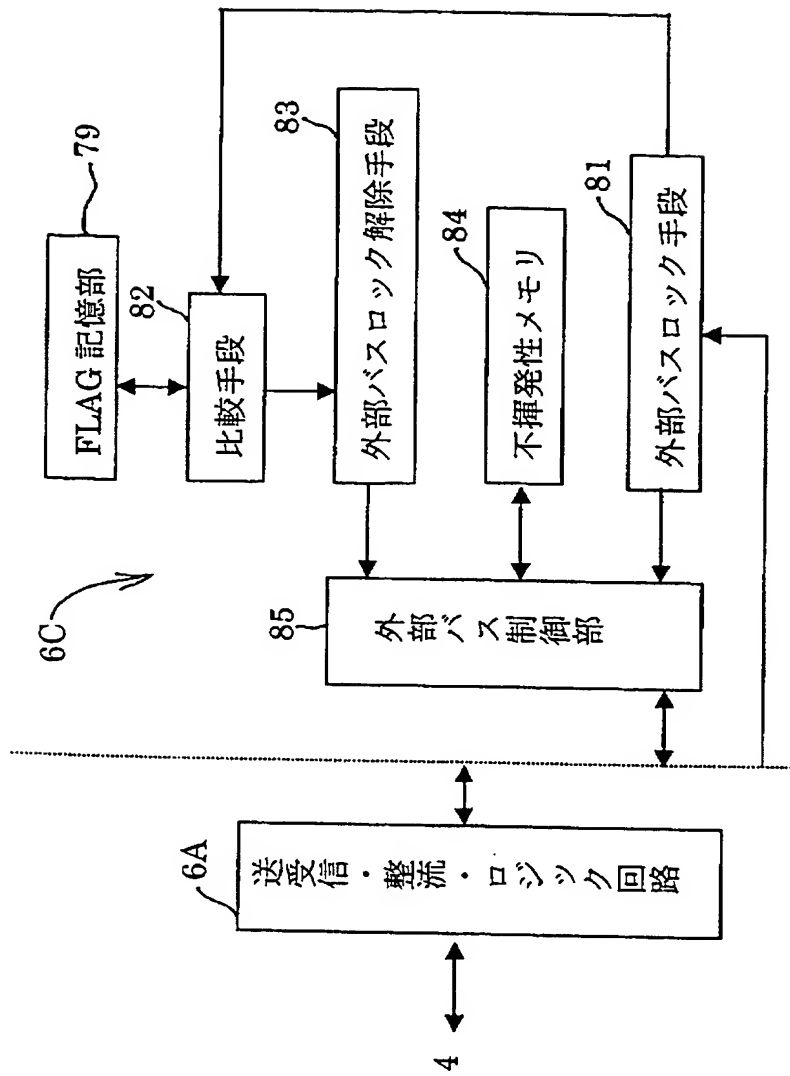
【図 4】



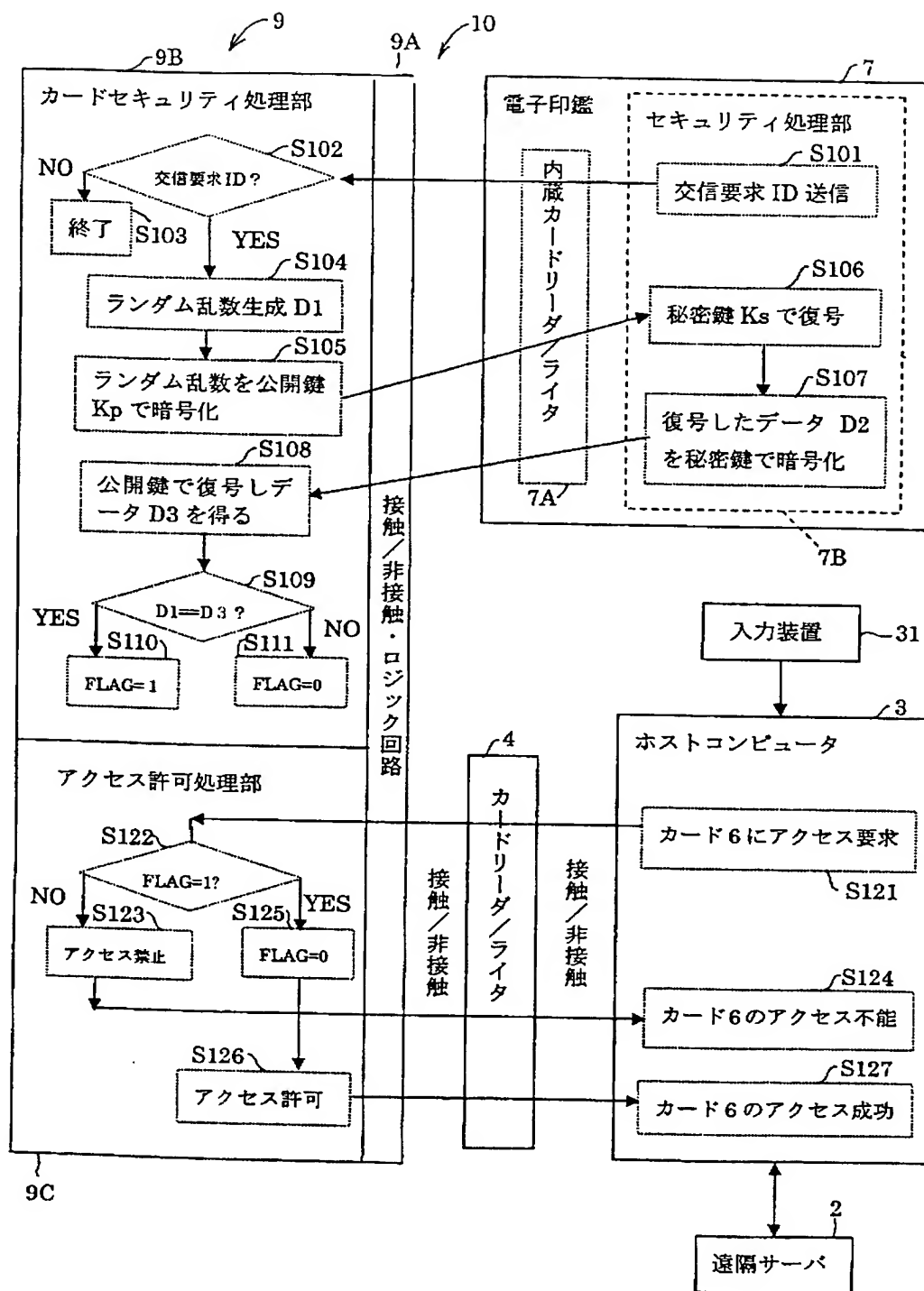
【図 5】



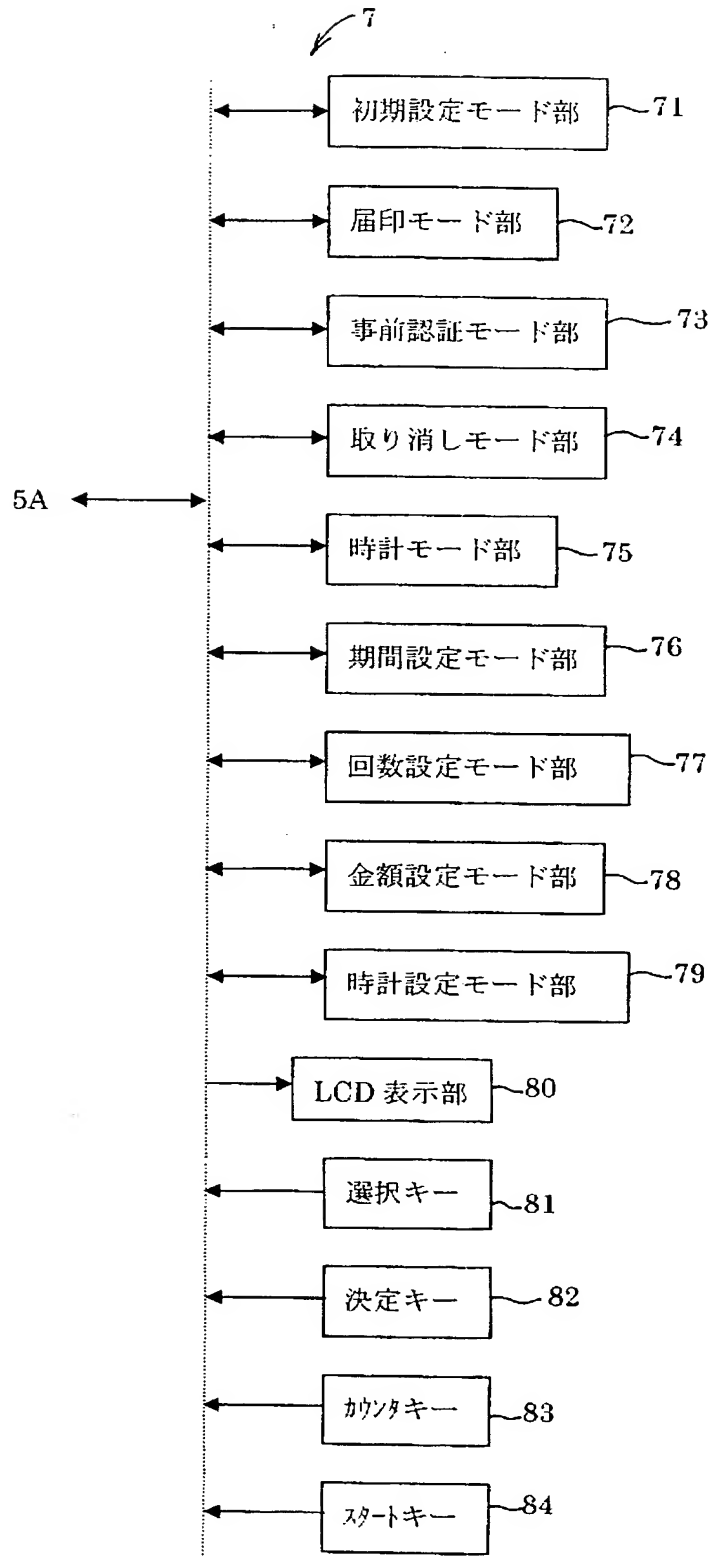
【図 6】



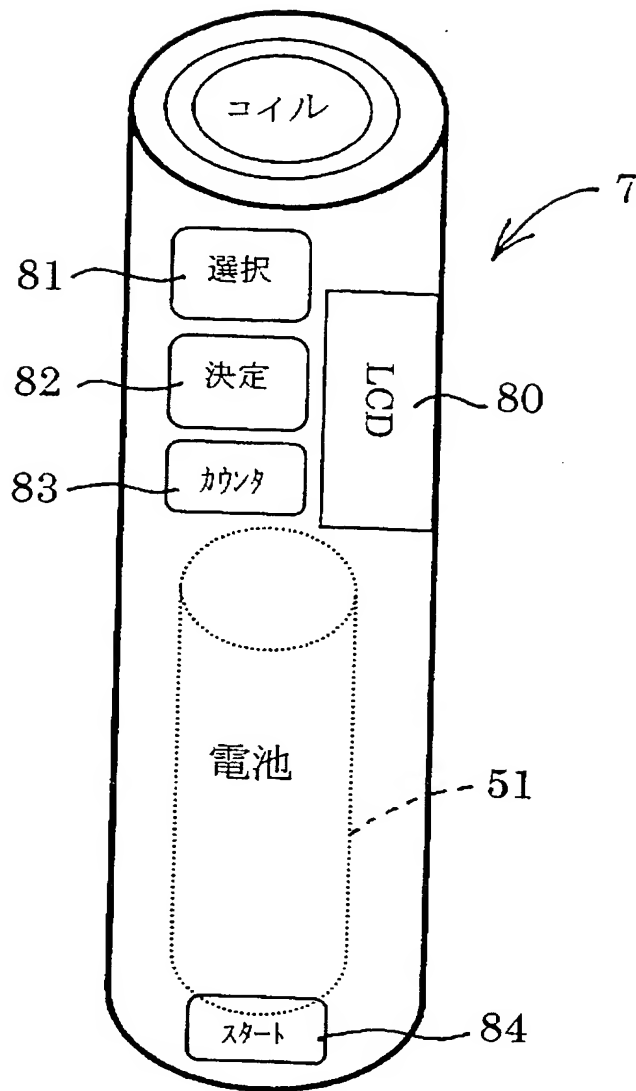
【図 7】



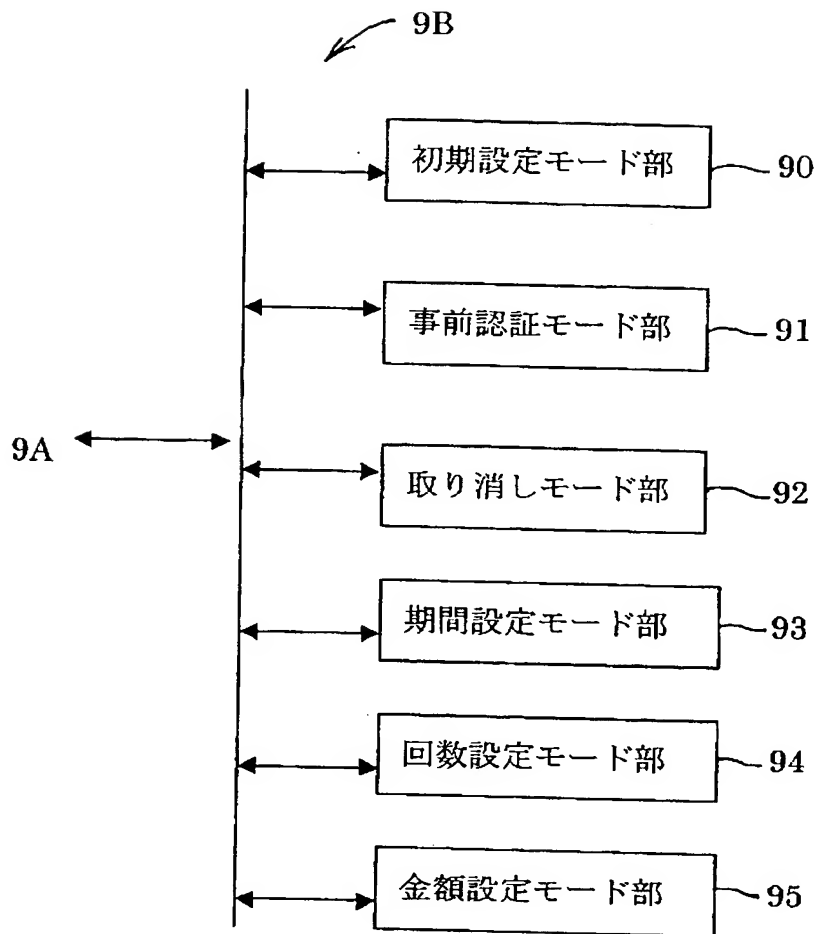
【図 8】



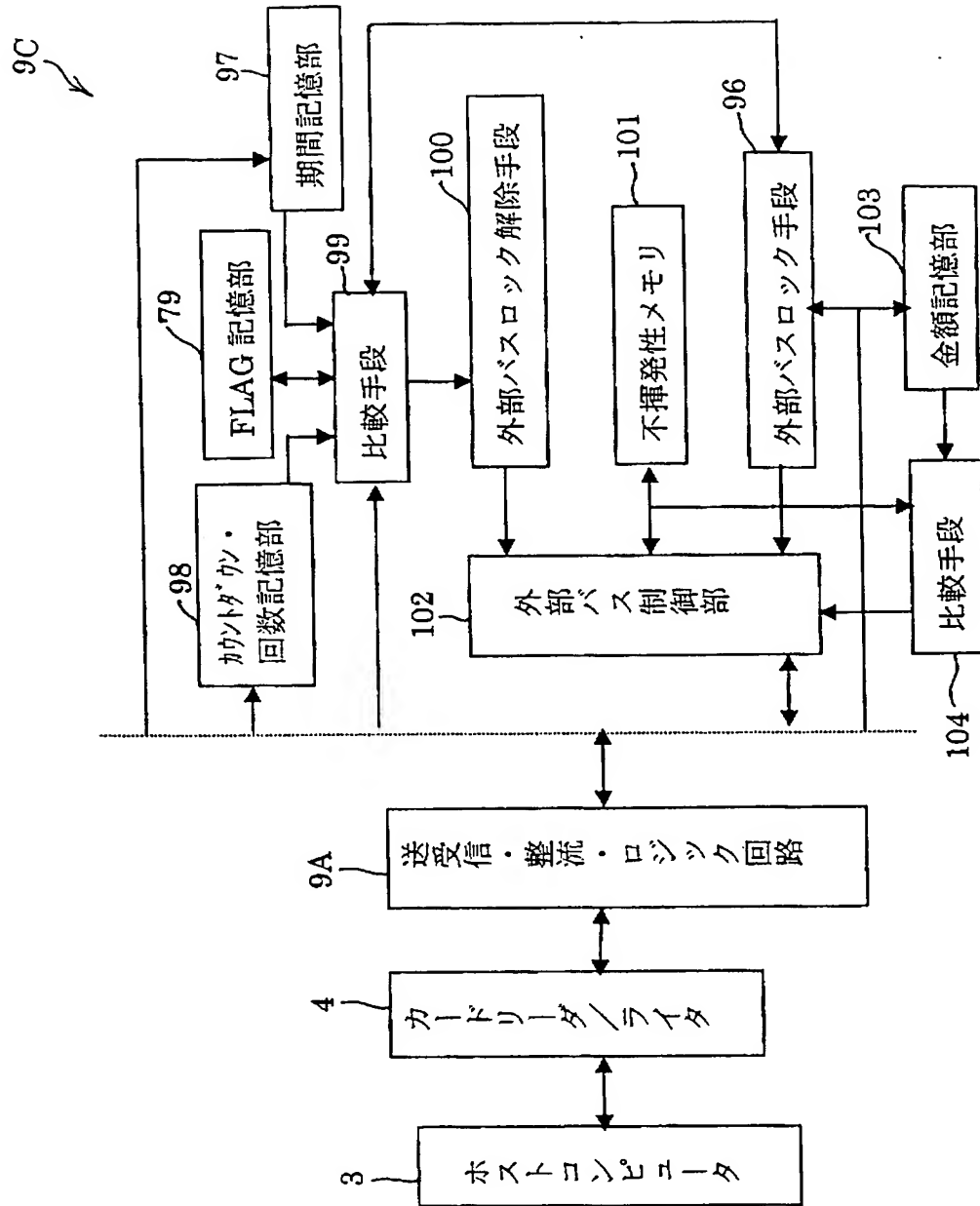
【図 9】



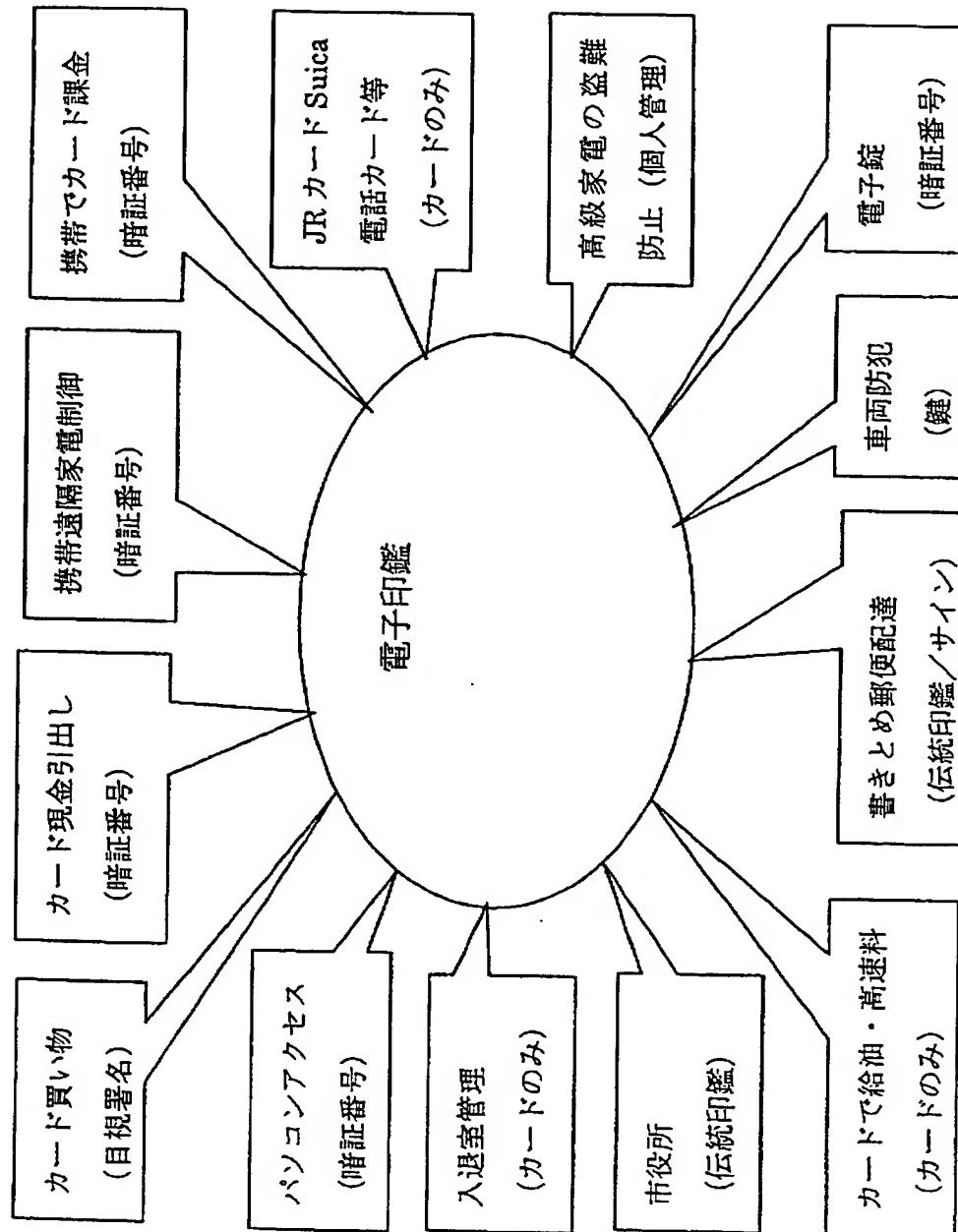
【図 10】



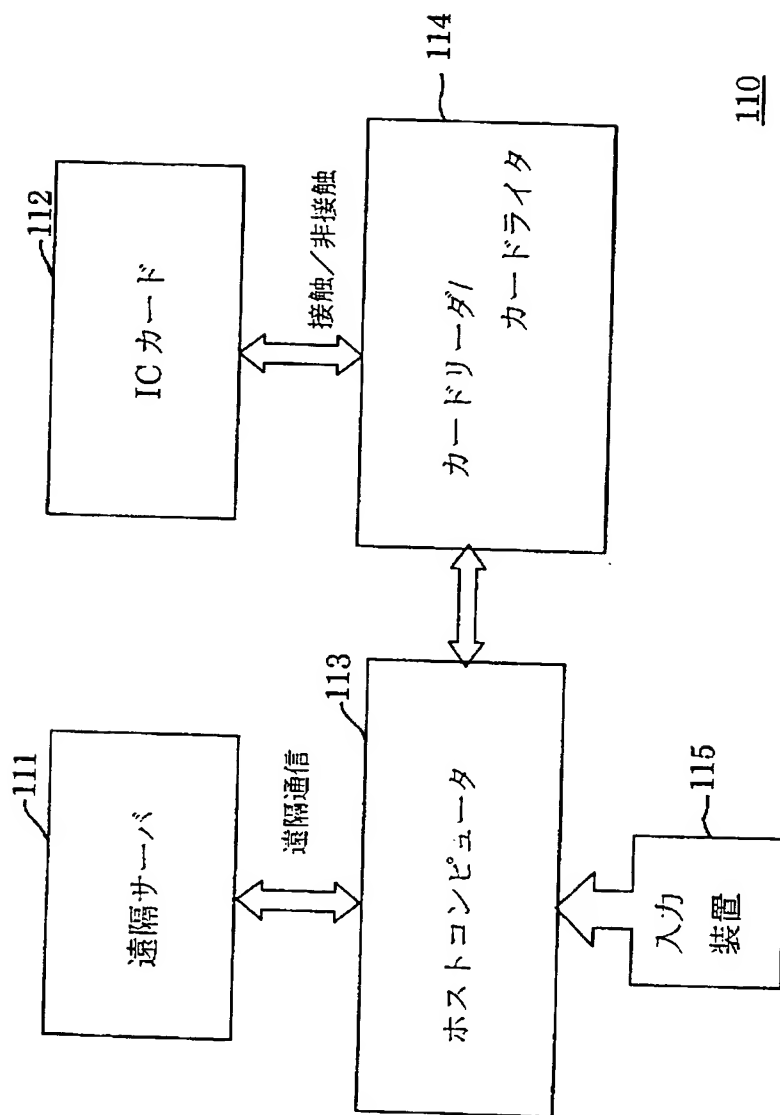
【図 11】



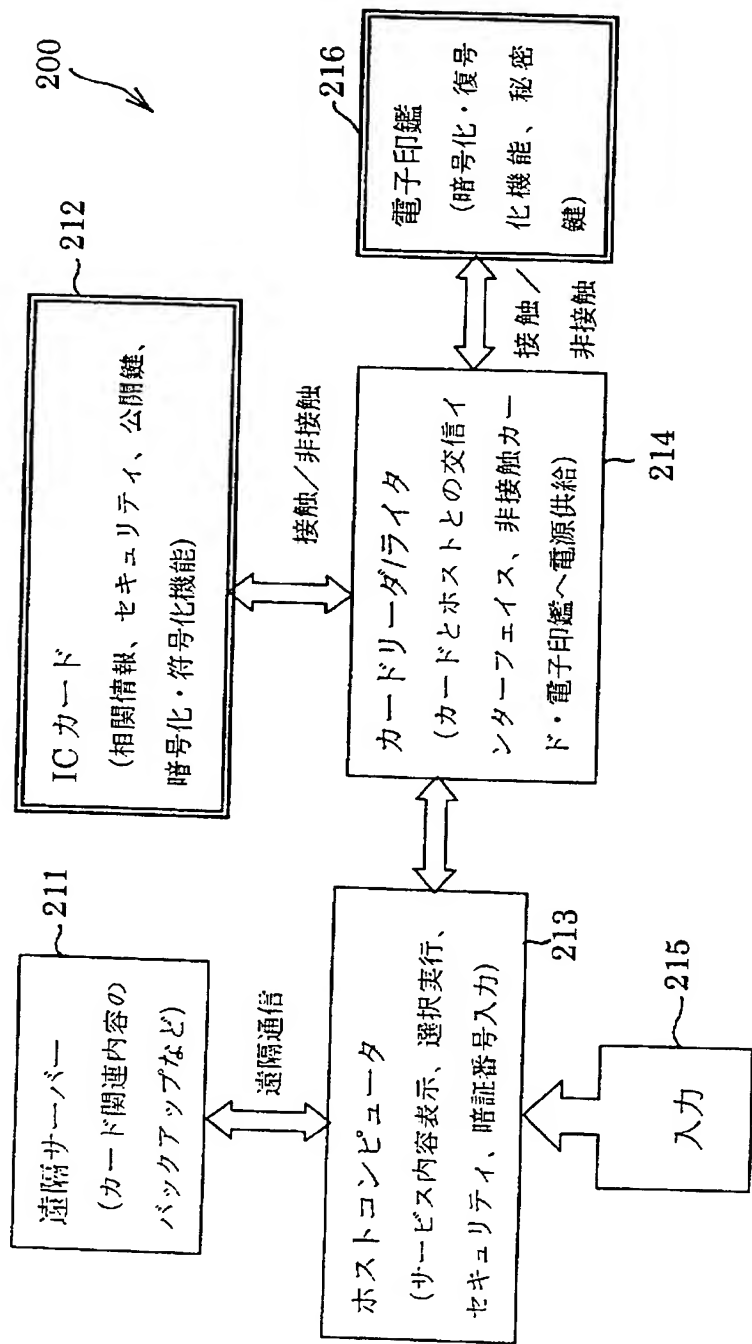
【図 12】



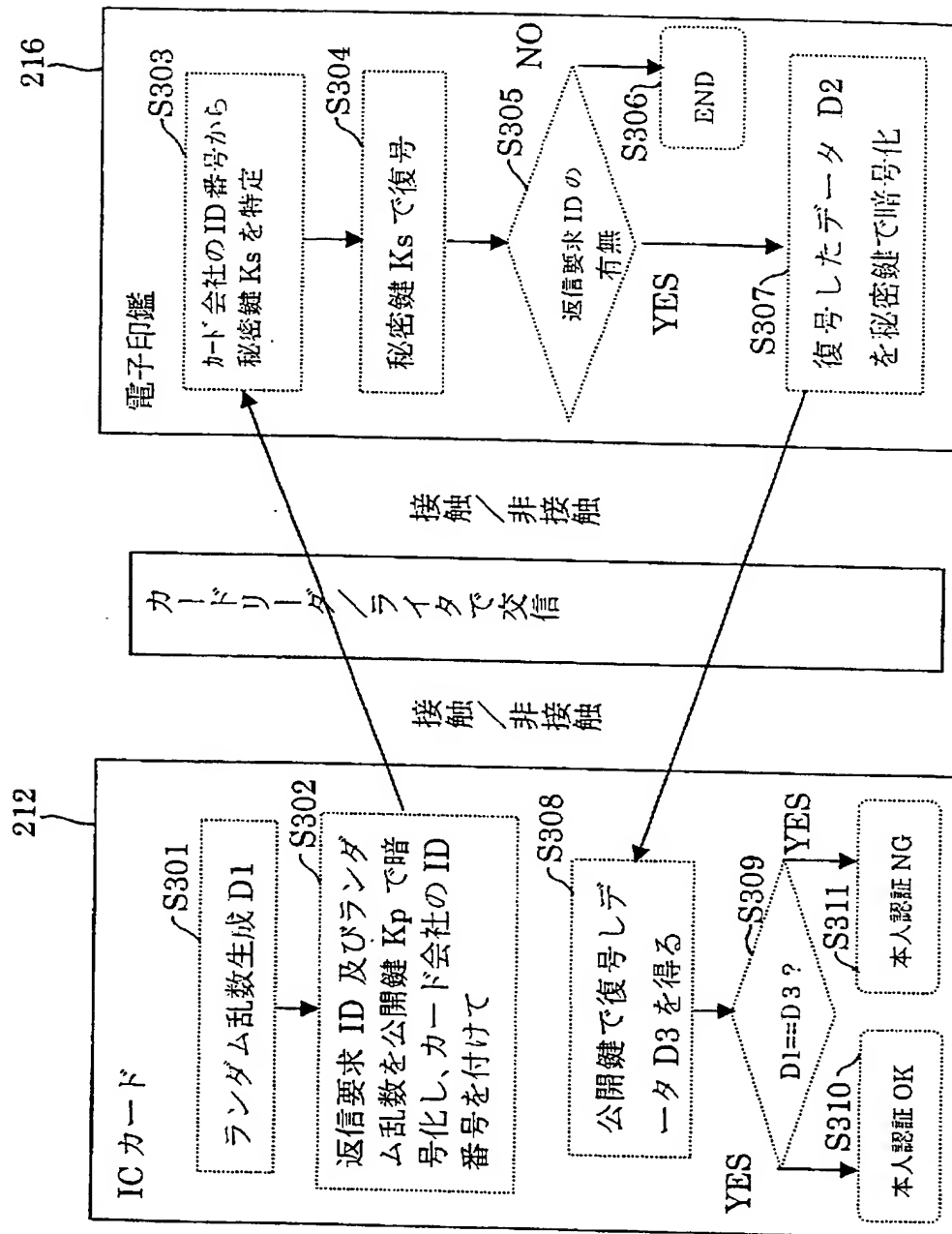
【図 13】



【図 14】



【図 15】



【書類名】 要約書

【要約】

【課題】 電子印鑑にカード会社の I D 番号を組み込むことなく、電子印鑑を届印としてカードに登録することにより、 I C カードを容易に発行でき、かつ、従来の電子印鑑を用いないシステムに対して新たなる改造や増設をすることなく、電子印鑑とカードによる事前の本人認証により処理相手に電子印鑑を渡さずに、電子印鑑を高セキュリティでカードのアクセス保護に使用できる。

【解決手段】 電子印鑑 5 または 7 側からカード 6 に対して交信要求 (I D) を送信し、カード 6 はこれをチェックする。チェックが O K であれば、カード 6 の事前認証部のカードセキュリティ処理部 6 B では、ランダム乱数を発生させ、これを公開鍵で暗号化して、電子印鑑 5 側に送り、電子印鑑 5 はこの受け取ったデータを秘密鍵で復号化し、さらに秘密鍵で暗号化してカード 6 に送る。このデータを受け取ったカード 6 は、又公開鍵で復号化する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2002-289228
受付番号	50201479190
書類名	特許願
担当官	第七担当上席 0096
作成日	平成 14 年 10 月 2 日

<認定情報・付加情報>

【特許出願人】

【識別番号】 000005049

【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号

【氏名又は名称】 シャープ株式会社

【代理人】 申請人

【識別番号】 100078282

【住所又は居所】 大阪市中央区城見 1 丁目 2 番 2 7 号 クリスタル
タワー 1 5 階

【氏名又は名称】 山本 秀策

【選任した代理人】

【識別番号】 100062409

【住所又は居所】 大阪府大阪市中央区城見 1 丁目 2 番 2 7 号 クリ
スタルタワー 1 5 階 山本秀策特許事務所

【氏名又は名称】 安村 高明

【選任した代理人】

【識別番号】 100107489

【住所又は居所】 大阪市中央区城見一丁目 2 番 2 7 号 クリスタル
タワー 1 5 階 山本秀策特許事務所

【氏名又は名称】 大塩 竹志

次頁無

特願 2 0 0 2 - 2 8 9 2 2 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 0 4 9]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

大阪府大阪市阿倍野区长池町 2 2 番 2 2 号

氏 名

シャープ株式会社